NETGEAR RangeMax™ NEXT Wireless Router WNR834B User Manual



NETGEAR, Inc.
4500 Great America Parkway
Santa Clara, CA 95054 USA

202-10171-02
January 2007

Product Registration, Support, and Documentation

Register your product at *http://www.NETGEAR.com/register.* Registration is required before you can use our telephone support service. Product updates and Web support are always available by going to: *http://kbserver.netgear.com/*.

Setup documentation is available on the CD, on the support website, and on the documentation website. When the wireless router is connected to the Internet, click the KnowledgeBase or the Documentation link under the Web Support menu to view support information.

Trademarks

NETGEAR and the NETGEAR logo are registered trademarks, and RangeMax and Smart Wizard are trademarks of NETGEAR. Inc. Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation. Other brand and product names are registered trademarks or trademarks of their respective holders.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice.

NETGEAR does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Certificate of the Manufacturer/Importer

It is hereby certified that the RangeMax NEXT Wireless Router WNR834B has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

Federal Office for Telecommunications Approvals has been notified of the placing of this equipment on the market and has been granted the right to test the series for compliance with the regulations.

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das RangeMax NEXT Wireless Router WNR834B gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z.B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

Das Bundesamt für Zulassungen in der Telekommunikation wurde davon unterrichtet, daß dieses Gerät auf den Markt gebracht wurde und es ist berechtigt, die Serie auf die Erfüllung der Vorschriften hin zu überprüfen.

Voluntary Control Council for Interference (VCCI) Statement

This equipment is in the second category (information equipment to be used in a residential area or an adjacent area thereto) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines aimed at preventing radio interference in such residential areas.

When used near a radio or TV receiver, it may become the cause of radio interference.

Read instructions for correct handling.

Regulatory Compliance Information

This section includes user requirements for operating this product in accordance with National laws for usage of radio spectrum and operation of radio devices. Failure of the end-user to comply with the applicable requirements may result in unlawful operation and adverse action against the end-user by the applicable National regulatory authority.

NOTE: This product's firmware limits operation to only the channels allowed in a particular Region or Country. Therefore, all options described in this user's guide may not be available in your version of the product.

Europe – EU Declaration of Conformity

Marking by the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC). This equipment meets the following conformance standards:

EN300 328, EN301 489-17, EN60950

A printed copy of the EU Declaration of Conformity certificate for this product is provided in the WNR834B product package.

Europe – Declaration of Conformity in Languages of the European Community

Cesky [Czech]	*NETGEAR* Inc. tímto prohlašuje, že tento Radiolan je ve shode se základními požadavky a dalšími príslušnými ustanoveními smernice 1999/5/ES..
Dansk [Danish]	Undertegnede *NETGEAR Inc.* erklærer herved, at følgende udstyr Radiolan overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt *NETGEAR Inc.*, dass sich das Gerät Radiolan in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab *NETGEAR Inc.* seadme Radiolan vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, *NETGEAR Inc.*, declares that this Radiolan is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]	Por medio de la presente *NETGEAR Inc.* declara que el Radiolan cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ *NETGEAR Inc.* ΔΗΛΩΝΕΙ ΟΤΙ Radiolan ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Français [French]	Par la présente *NETGEAR Inc.* déclare que l'appareil Radiolan est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [Italian]	Con la presente *NETGEAR Inc.* dichiara che questo Radiolan è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.

Latviski [Latvian]	Ar šo *NETGEAR Inc.* deklarē, ka Radiolan atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo *NETGEAR Inc.* deklaruoja, kad šis Radiolan atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [Dutch]	Hierbij verklaart *NETGEAR Inc.* dat het toestel Radiolan in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
Malti [Maltese]	Hawnhekk, *NETGEAR Inc.*, jiddikjara li dan Radiolan jikkonforma mal-htigijiet essenzjali u ma provvedimenti ohrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, *NETGEAR Inc.* nyilatkozom, hogy a Radiolan megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Polski [Polish]	Niniejszym NETGEAR Inc. oświadcza, że Radiolan jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	*NETGEAR Inc.* declara que este Radiolan está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	NETGEAR Inc. izjavlja, da je ta Radiolan v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	*NETGEAR Inc.* týmto vyhlasuje, _e Radiolan spĺňa základné po_iadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	*NETGEAR Inc.* vakuuttaa täten että Radiolan tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]	Härmed intygar *NETGEAR Inc.* att denna Radiolan står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
Íslenska [Icelandic]	Hér með lýsir *NETGEAR Inc.* yfir því að Radiolan er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.
Norsk [Norwegian]	*NETGEAR Inc.* erklærer herved at utstyret *Radiolan* er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.

FCC Requirements for Operation in the United States

FCC Information to User

This product does not contain any user serviceable components and is to be used with approved antennas only. Any product changes or modifications will invalidate all applicable regulatory certifications and approvals

FCC Guidelines for Human Exposure

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20 cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Declaration Of Conformity

We NETGEAR, Inc., 4500 Great America Parkway, Santa Clara, CA 95054, declare under our sole responsibility that the model WNR834B RangeMax NEXT Wireless Router WNR834B complies with Part 15 of FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

FCC Radio Frequency Interference Warnings & Instructions

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following methods:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and the receiver
- Connect the equipment into an electrical outlet on a circuit different from that which the radio receiver is connected
- Consult the dealer or an experienced radio/TV technician for help.

RangeMax NEXT Wireless Router WNR834B

FC

Tested to Comply
with FCC Standards
FOR HOME OR OFFICE USE
PY306XXXXXX

Modifications made to the product, unless expressly approved by NETGEAR, Inc., could void the user's right to operate the equipment.

Maximum Wireless Signal Rate Derived from IEEE Standard 802.11 Specifications

Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate.

Product and Publication Details

Model Number:	WNR834B
Publication Date:	January 2007
Product Family:	Wireless Router
Product Name:	RangeMax NEXT Wireless Router WNR834B
Home or Business Product:	Home
Language:	English
Publication Part Number:	202-10171-02

Contents

NETGEAR RangeMax™ NEXT Wireless Router WNR834B User Manual

Chapter 1
About This Manual

The user manual provides information for configuring the features of the RangeMax NEXT Wireless Router WNR834B beyond initial configuration settings. Initial configuration instructions can be found in the *NETGEAR Wireless Router Setup Manual*. You should have basic to intermediate computer and Internet skills.

Conventions, Formats and Scope

The conventions, formats, and scope of this manual are described in the following paragraphs:

- **Typographical Conventions.** This manual uses the following typographical conventions:

Italics	Emphasis, books, CDs, URL names
Bold	User input
`Fixed`	Screen text, file and server names, extensions, commands, IP addresses

- **Formats.** This manual uses the following formats to highlight special messages:

Note: This format is used to highlight information of importance or special interest.

Tip: This format is used to highlight a procedure that will save time or resources.

Warning: Ignoring this type of note may result in a malfunction or damage to the equipment, a breach of security, or a loss of data.

Danger: This is a safety warning. Failure to take heed of this notice may result in personal injury or death.

- **Scope.** This manual is written for the WNR834B router according to these specifications:

Product Version	RangeMax NEXT Wireless Router WNR834B
Manual Publication Date	January 2007

For more information about network, Internet, firewall, and VPN technologies, see the links to the NETGEAR website in Appendix B, "Related Documents".

Note: Product updates are available on the NETGEAR, Inc. website at *http://kbserver.netgear.com/products/WNR834B.asp*.

How to Use This Manual

The HTML version of this manual includes the following:

- Buttons, [>] and [<], for browsing forwards or backwards through the manual one page at a time
- A [table of contents] button that displays the table of contents and an [index] button. Double-click on a link in the table of contents or index to navigate directly to where the topic is described in the manual.
- A [knowledge base] button to access the full NETGEAR, Inc. online knowledge base for the product model.
- Links to PDF versions of the full manual and individual chapters.

How to Print this Manual

To print this manual, you can choose one of the following options, according to your needs.

- **Printing a Page from HTML**. Each page in the HTML version of the manual is dedicated to a major topic. Select File > Print from the browser menu to print the page contents.

- **Printing from PDF**. Your computer must have the free Adobe Acrobat reader installed in order to view and print PDF files. The Acrobat reader is available on the Adobe Web site at *http://www.adobe.com*.
  - **Printing a PDF Chapter.** Use the *PDF of This Chapter* link at the top left of any page.
    - Click the *PDF of This Chapter* link at the top left of any page in the chapter you want to print. The PDF version of the chapter you were viewing opens in a browser window.
    - Click the print icon in the upper left of your browser window.
  - **Printing a PDF version of the Complete Manual**. Use the *Complete PDF Manual* link at the top left of any page.
    - Click the *Complete PDF Manual* link at the top left of any page in the manual. The PDF version of the complete manual opens in a browser window.
    - Click the print icon in the upper left of your browser window.

Tip: If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature.

Revision History

NETGEAR, Inc. is constantly searching for ways to improve its products and documentation. The following table indicates any changes that may have been made since the WNR834B router was introduced.

Table 1-1. Publication Revision History

Version	Date	Description
v1.0	April 2006	Original publication.
v1.2	January 2007	Restructure.

Chapter 2
Configuring Basic Connectivity

This chapter describes the parameters for your Internet connection and your wireless local area network (LAN) connection. When you perform the initial configuration of your wireless router using the *Resource CD* as described in the *NETGEAR Wireless Router Setup Manual*, these parameters are configured automatically for you. This chapter provides further details about these connectivity settings, as well as instructions on how to log in to the rouer for further configuration.

Note: NETGEAR recommends using the Smart Wizard on the *Resource CD* for initial configuration, as described in the *NETGEAR Wireless Router Setup Manual*.

This chapter includes:

- Using the Setup Manual
- Accessing the Wireless Router For Configuration
- Configuring Your Internet Connection Using the Smart Setup Wizard
- Configuring Wireless Settings

Using the Setup Manual

For first-time installation of your wireless router, refer to the *NETGEAR Wireless Router Setup Manual*. The Setup Manual explains how to launch the NETGEAR Smart Wizard on the *Resource CD* to step you through the procedure to connect your router, modem, and computers. The Smart Wizard will assist you in configuring your wireless settings and enabling wireless security for your network. After initial configuration using the Setup Manual, you can use the information in this User Manual to configure additional features of your wireless router.

For installation instructions in a language other than English, refer to the language options on the *Resource CD*, or refer to one of the online versions listed in the following table.

Table 2-1. RangeMax NEXT Wireless Router WNR834B Online Setup Manuals

Language	Setup Manual URL
English	*http://documentation.netgear.com/wnr834b/enu/208-10070-01/*
German	*http://documentation.netgear.com/wnr834b/deu/208-10132-01/*
French	*http://documentation.netgear.com/wnr834b/fra/208-10130-01/*
Italian	*http://documentation.netgear.com/wnr834b/ita/208-10071-01/*
Spanish	*http://documentation.netgear.com/wnr834b/esp/208-10131-01/*
Dutch	*http://documentation.netgear.com/wnr834b/nld/208-10072-01/*
Swedish	*http://documentation.netgear.com/wnr834b/sve/208-10073-01/*

Accessing the Wireless Router For Configuration

When the wireless router is connected to your network, you can access it for configuration using your browser. Follow these instructions to access the Web Configuration Manager:

1. Connect to the wireless router by typing **http://www.routerlogin.net** or the router's LAN IP address (default is 192.168.1.1) in the address field of your browser and then pressing Enter. A login window opens:.



Figure 2-1

	Tip: You can connect to the wireless router by typing either of these URLs in the address field of your browser and then pressing Enter: • *http://www.routerlogin.net* • *http://www.routerlogin.com* If these URLs do not work, you must type the IP address of the router, such as: • *http://192.168.1.1*

2. Enter **admin** for the router user name and your password (or the default, **password**). To change the password, see "Changing the Administrator Password" on page 3-14.

	Note: The router user name and password are not the same as any user name or password you may use to log in to your Internet connection.

Once you have entered a user name and password, your Web browser displays the wireless router’s home page.

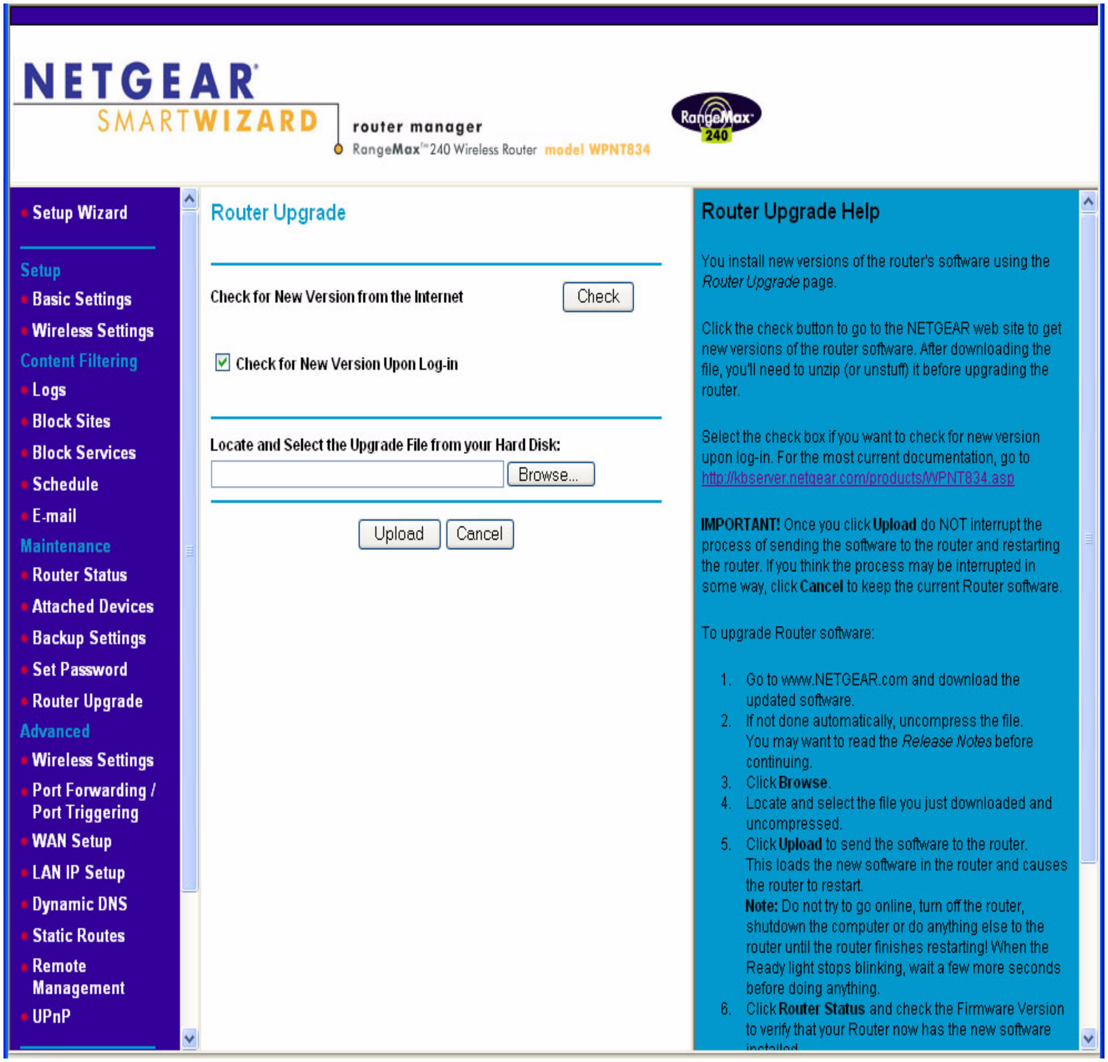


Figure 2-2

	Note: If the Check for New Version Upon Log-in checkbox is selected, the home page will be the Router Upgrade page. Otherwise, it will be the Basic Settings page.

If the wireless router is connected to the Internet, you can click the Knowledge Base or the Documentation link under the Web Support menu to view support information or the documentation for the wireless router.

If you do not click Logout, the wireless router will wait 5 minutes after there is no activity before it automatically logs you out.

Configuring Your Internet Connection Using the Smart Setup Wizard

You can manually configure your Internet connection using the Basic Settings menu, or you can allow the Smart Setup Wizard to determine your Internet Service Provider (ISP) configuration.

The Smart Setup Wizard searches your Internet connection for servers and protocols to determine your ISP configuration. This feature is not the same as the Smart Wizard configuration assistant that only appears when the router is in its factory default state. To use the Smart Setup Wizard to assist with configuration or to verify the Internet connection settings, follow this procedure:

1. From the top of the main menu of the browser interface, click Setup Wizard.
2. Click Next to proceed. Input your ISP settings, as needed.
3. At the end of the Setup Wizard, click Test to verify your Internet connection. If you have trouble connecting to the Internet, see Chapter 8, “Troubleshooting”.

Viewing and Configuring Basic ISP Settings

Parameters related to your Internet service are configured in the Basic Settings menu. To access the Basic Settings menu:

1. From the main menu of the router’s Web configuration interface, under the Setup heading, click Basic Settings.

The content you see in the Basic Settings menu depends on whether your ISP requires that you log in with a user name and password for Internet access.

No Login Required by ISP

If no login is required by your ISP, the following parameters appear in the Basic Settings menu..

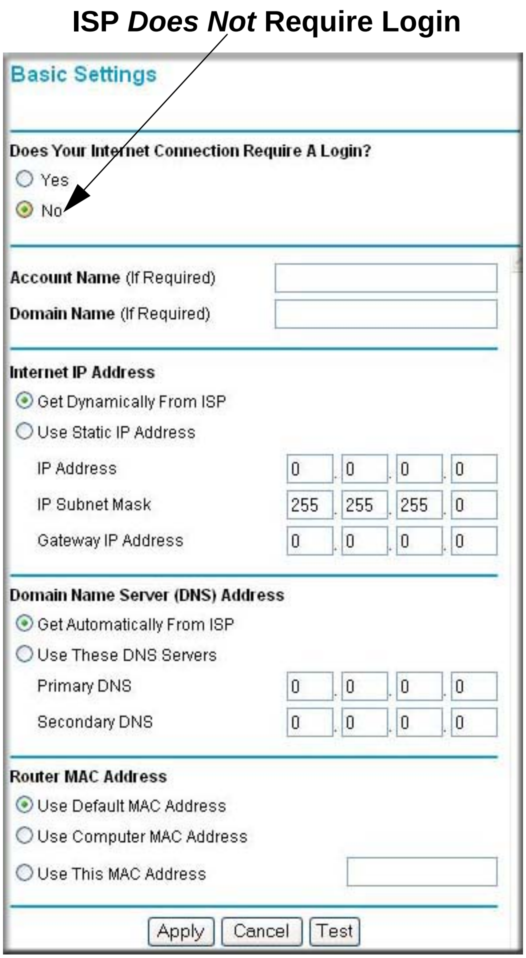


Figure 2-3

- Account Name (may also be called Host Name)
  The account name will be provided to the ISP during a DHCP request from your router. In most cases, this parameter is not required, but some ISPs require it for access to ISP services such as mail or news servers.

- Domain Name.
  The domain name will be provided by your router to computers on your LAN when the computers request DHCP settings from your router. In most cases, this parameter is not required.
- Internet IP Address
  Determines how your router obtains an IP address for Internet access.
  — If your ISP assigns an IP address dynamically (by DHCP), select Get Automatically.
  — If your ISP has assigned you a permanent, fixed (static) IP address for your computer, select Use Static IP Address. Enter the IP address that your ISP assigned. Also, enter the Subnet mask and the Gateway IP address. The Gateway is the ISP's router to which your router will connect.
- Domain Name Server (DNS) Address
  If you know that your ISP does not automatically transmit DNS addresses to the router during login, select Use These DNS Servers and enter the IP address of your ISP's Primary DNS Server. If a Secondary DNS Server address is available, enter it also.

Note: If you enter or change a DNS address, restart the computers on your network so that these settings take effect.

- Router's MAC Address
  This section determines the Ethernet MAC address that the router will use on the Internet port. Some ISPs (especially cablemodem providers) will register the Ethernet MAC address of the network interface card in your computer when your account is first opened. They will then only accept traffic from the MAC address of that computer. This feature allows your router to masquerade as that computer by "cloning" or "spoofing" its MAC address.

  To change the MAC address, choose one of the following methods:
  — Select Use Computer MAC Address. The router will then capture and use the MAC address of the computer that you are now using. You must be using the one computer that is allowed by the ISP.
  — Select Use this MAC address and type it in here.

Login Required by ISP

If you normally must use a login program such as WinPOET in order to access the Internet, your Internet connection requires a login. After you select Login Required, your Basic Settings menu will appear, as shown in the figure below.

→	**Note:** After you finish setting up your router, you will no longer need to launch the ISP's login program on your computer to access the Internet. When you start an Internet application, your router will automatically log you in.

If a login is required by your ISP, the following parameters appear in the Basic Settings menu:.

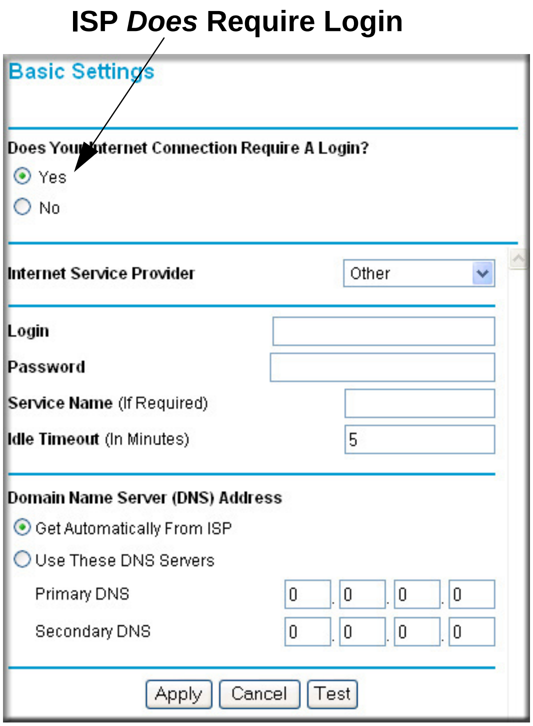


Figure 2-4

- Internet Service Provider
  This drop-down list.contains a few ISPs that need special protocols for connection. The list includes:
  - — PPTP (Point to Point Tunneling Protocol), used primarily in Austrian DSL services

— Telstra Bigpond, an Australian residential cablemodem service.

➡	**Note:** The Telstra Bigpond setting is only for older cablemodem service accounts still requiring a Bigpond Login utility. Telstra has discontinued this type of account. Those with Telstra DSL accounts and newer cablemodem accounts should select No for "Does Your Internet Connection Require a Login?"

— Other, which selects PPPoE (Point to Point Protocol over Ethernet), the protocol used by most DSL services worldwide

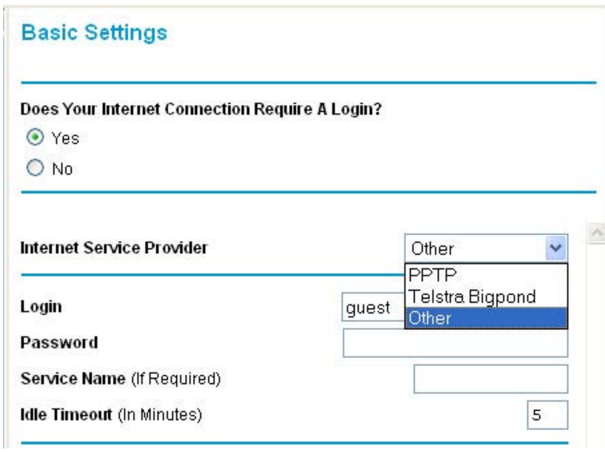


Figure 2-5

➡	**Note:** Not all ISPs are listed here. The ones on this list have special requirements.

- Login and Password
  This is the user name and password provided by your ISP. This name and password will be used to log in to the ISP server.
- Service Name
  If your connection is capable of connecting to multiple Internet services, this parameter specifies which service to use.

- Idle Timeout
  Your Internet connection will be logged out if there is no data transfer during the specified time interval.
- Domain Name Server (DNS) Address
  If you know that your ISP does not automatically transmit DNS addresses to the router during login, select Use These DNS Servers and enter the IP address of your ISP's Primary DNS Server. If a Secondary DNS Server address is available, enter it also.

> **Note:** If you enter or change a DNS address, restart the computers on your network so that these settings take effect.

Configuring Wireless Settings

This section explains the general wireless settings of the WNR834B. Configuration of the security-related wireless features is explained in greater detail in "Choosing Appropriate Wireless Security" on page 3-1.

The WNR834B provides two menus for configuring the wireless settings. The basic Wireless Settings menu link is located under the Setup heading in the main menu of the browser interface. The Advanced Wireless Settings menu link is located under the Advanced heading.

Viewing the Basic Wireless Settings

To view the basic wireless settings:

- From the main menu of the browser interface, under Setup, click Wireless Settings.

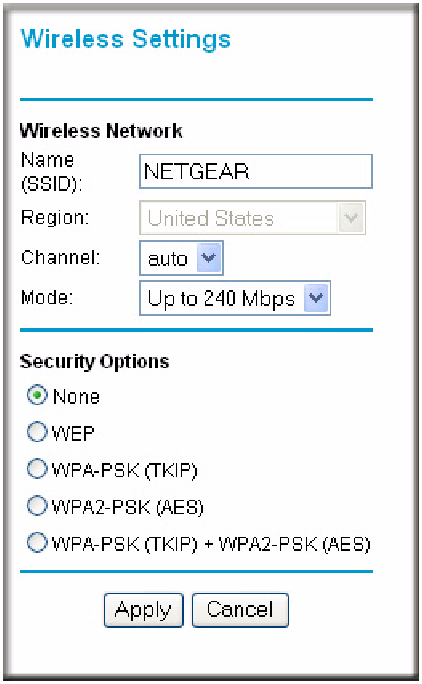


Figure 2-6

The available settings in this menu are:

- Name (SSID)
  The SSID is also known as the wireless network name. Enter a value of up to 32 alphanumeric characters. When more than one wireless network is active, different wireless network names provide a way to separate the traffic. For a wireless device to participate in a particular wireless network, it must be configured with the SSID for that network. The WNR834B default SSID is **NETGEAR**.
- Region
  This field identifies the region where the WNR834B can be used. It may not be legal to operate the wireless features of the wireless router in a region other than one of those identified in this field.

Note: The region selection feature may not be available in all countries.

- Channel
  This field determines which operating frequency is used. It should not be necessary to change the wireless channel unless you notice interference problems with another nearby wireless network. For more information on the wireless channel frequencies, see “Wireless Communications” in Appendix B.
- Mode
  This field determines which data communications protocol is used. You can choose from:
  - g only
    Dedicates the WNR834B to communicating with the higher bandwidth 802.11g wireless devices exclusively.
  - g and b
    Provides backward compatibility with the slower 802.11b wireless devices while still enabling 802.11g communications.
  - Up To 126 Mbps
    Provides two transmission streams with different data on the same channel at the same time.
  - Up To 240 Mbps
    Uses channel expansion to achieve the 240 Mbps data rate. The WNR834B router will use the channel you selected as the primary channel and expand to the secondary channel (primary channel +4 or –4) to achieve a 40MHz frame-by-frame bandwidth. The WNR834B router will detect channel usage and will disable frame-by-frame expansion if the expansion would result in interference with the data transmission of other access points or clients.

> **Note:** The maximum wireless signal rate is derived from the IEEE Standard 802.11 Specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate.

- Security Options
  The selection of wireless security options can significantly affect your network performance. The time it takes to establish a wireless connection can vary depending on both your security settings and router placement. WEP connections can take slightly longer to establish. Also, WEP, WPA-PSK and WPA2-PSK encryption can consume more battery power on a notebook computer, and can cause significant performance degradation with a slow computer. Instructions for configuring the security options can be found in “Choosing Appropriate Wireless Security” on page 3-1. A full explanation of wireless security standards is available in “Wireless Communications” in Appendix B.

Viewing the Advanced Wireless Settings

To view the advanced wireless settings:

From the main menu of the browser interface, under Advanced, click Wireless Settings.

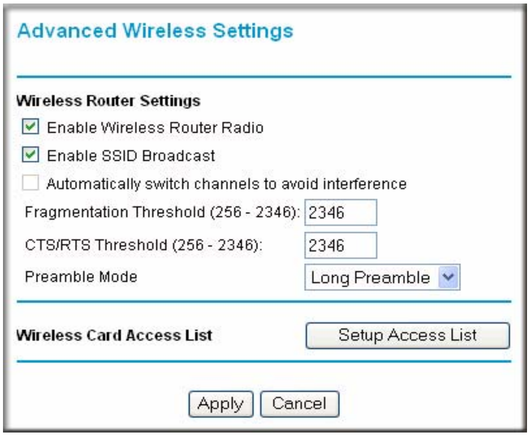


Figure 2-7

The available settings in this menu are:

- Enable Wireless Router Radio
  If you disable the wireless router radio, wireless devices cannot connect to the WNR834B.
- Enable SSID Broadcast
  If you disable broadcast of the SSID, only devices that know the correct SSID can connect. Disabling SSID broadcast nullifies the wireless network 'discovery' feature of some products, such as Windows XP.
- Automatically switch channels to avoid interference
  Select this checkbox to have the WNR834B router periodically survey the wireless environment to ensure that it is using the clearest channel. If a clearer channel is available, it might automatically switch channels.

Note: After the router switches channels, there could be a slight delay while your wireless computers reconnect to the router. To avoid this possibility, leave this checkbox unselected.

- Wireless Card Access List
  When a Wireless Card Access List is configured and enabled, the WNR834B checks the MAC address of any wireless device attempting a connection, and only allows connections to computers identified on the trusted computers list. For instructions on configuring the Wireless Card Access List, see "Restricting Wireless Access by MAC Address" on page 3-12.

Note: The Fragmentation Threshold, CTS/RTS Threshold and Preamble Mode options are reserved for wireless testing and advanced configuration only. Do not change these settings.

Chapter 3
Safeguarding Your Network

The RangeMax NEXT Wireless Router WNR834B provides highly effective security features which are covered in detail in this chapter.

This chapter includes:

- Choosing Appropriate Wireless Security
- Configuring WEP Wireless Security
- Configuring WPA-PSK or WPA2-PSK Wireless Security
- Restricting Wireless Access by MAC Address
- Changing the Administrator Password
- Backing Up Your Configuration
- Understanding Your Firewall

Choosing Appropriate Wireless Security

Unlike wired network data, anyone with a compatible adapter can receive your wireless data transmissions well beyond your walls. Operating an unsecured wireless network creates an opportunity for outsiders to eavesdrop on your network traffic or to enter your network to access your computers and files. For this reason, use the security features of your wireless equipment. Deploy the security features appropriate to your needs.

Note: Indoors, computers can connect over 802.11b/g wireless networks at ranges of up to 300 feet. Such distances can allow for others outside of your immediate area to access your network.

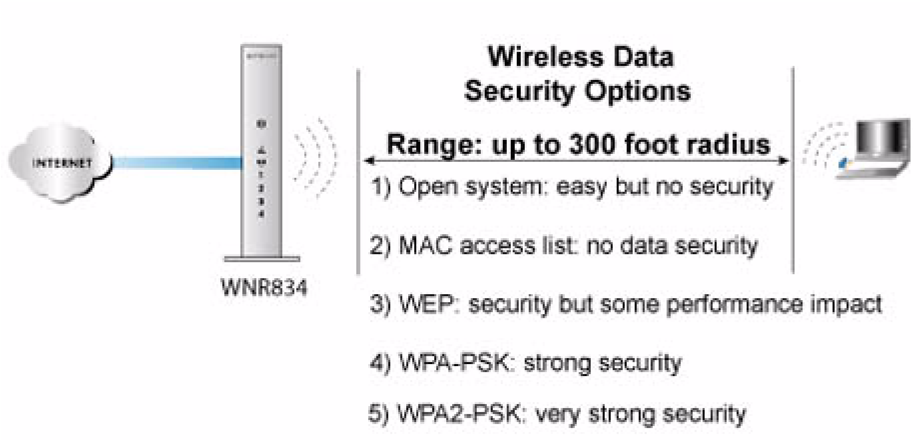


Figure 3-1

There are several ways you can enhance the security of your wireless network. In order of increasing effectiveness:

- **Turn Off the Broadcast of the Wireless Network Name SSID.** If you disable the broadcast of the SSID, only devices that know the correct SSID can connect. This nullifies the wireless network 'discovery' feature of some products such as Windows XP, but your data is still fully exposed to an intruder using available wireless eavesdropping tools.
- **Restrict Access Based on MAC Address.** You can restrict access to only trusted computers so that unknown computers cannot wirelessly connect to the WNR834B. MAC address filtering adds an obstacle against unwanted access to your network by the general public, but the data broadcast over the wireless link is fully exposed. This data includes your trusted MAC addresses, which can be read and impersonated by a hacker.
- **WEP.** Wired Equivalent Privacy (WEP) data encryption provides moderate data security. WEP Shared Key authentication and WEP data encryption can be defeated by a determined eavesdropper using publicly available tools.
- **WPA-PSK** and **WPA2-PSK.** Wi-Fi Protected Access with Pre-Shared Key (WPA-PSK and WPA2-PSK) data encryption provides extremely strong data security, very effectively blocking eavesdropping. Because WPA and WPA2 are relatively new standards, older wireless adapters and devices may not support them. Check whether newer drivers are available from the manufacturer.
- **Turn Off the Wireless LAN.** If you disable the wireless LAN, wireless devices cannot communicate with the router at all. You might choose to turn off the wireless LAN when you are away or when other users of your network all use wired connections.

The time it takes to establish a wireless connection can vary depending on both your security settings and router placement. WEP connections can take slightly longer to establish. Also, WEP, WPA-PSK and WPA2-PSK encryption can consume more battery power on a notebook computer, and can cause significant performance degradation with a slow computer. For more details on wireless security methods, please see "Wireless Communications" in Appendix B.

Recommended Security Settings

Stronger security methods can entail a cost in terms of throughput, latency, battery consumption, and equipment compatibility. In choosing an appropriate security level, you can also consider the effort versus the reward for a hacker to break into your network. As a minimum, however, NETGEAR recommends using WEP with Shared Key authentication. Do not run an unsecured wireless network unless it is your intention to provide free Internet access for the public.

In addition, be sure to change the administration password of your router. Default passwords are well-known, and an intruder can use your administrator access to read or disable your security settings. To change the administrator password, see "Changing the Administrator Password" on page 3-14.

Changing Wireless Security Settings

This section describes the security-related wireless settings. For details on the configuration of the general wireless settings, see "Configuring Wireless Settings" on page 2-10.

To configure the wireless security settings of your router:

1. Log in to the WNR834B router at its default LAN address of *www.routerlogin.net* (or `192.168.1.1`) with its default user name of **admin** and default password of **password**, or using whatever LAN IP address and password you have set up.

2. From the main menu of the browser interface, under Setup, click Wireless Settings. The Wireless Settings menu appears.

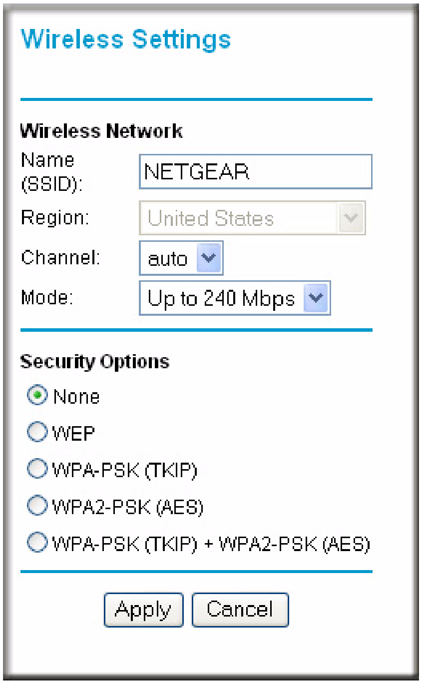


Figure 3-2

The available settings in this menu are:

- Name (SSID)
  The SSID, also known as the wireless network name, is broadcast by the wireless router so that nearby wireless devices can discover your network. You can disable this broadcast as described in "Configuring Security in the Advanced Wireless Settings Menu" on page 3-6.
- Region
  This field identifies the region where the WNR834B can be used.
- Channel
  This field determines which operating frequency is used.
- Mode
  This field determines which 802.11 data communications protocol is used.

- Security Options
  These options are the wireless security features you can enable. Table 3-1 identifies the basic wireless security options. For a detailed explanation of these standards, see "Wireless Communications" in Appendix B.

➡	**Note:** The Security Options displayed in this menu may change depending on the current selection of Wireless Mode.

Table 3-1. Basic Wireless Security Options

Field	Description
None	No wireless security. Only recommended for troubleshooting wireless connectivity.
WEP	WEP offers the following options: • Open System With Open Network authentication and 64- or 128-bit WEP Data Encryption, the WNR834B *does* perform data encryption but *does not* perform any authentication. Anyone can join the network. This setting provides very little practical wireless security. • Shared Key With Shared Key authentication, a wireless device must know the WEP key in order to join the network. Choose the Encryption Strength (64- or 128-bit data encryption). Manually enter the key values or enter a word or group of printable characters in the Passphrase box. Manually entered keys *are not* case sensitive but passphrase characters *are* case sensitive. **Note**: Not all wireless adapter configuration utilities support passphrase key generation. • Auto The wireless router automatically detects whether Open System or Shared Key is used.
WPA-PSK **WPA2-PSK**	WPA-Pre-shared Key *does* perform authentication. WPA-PSK uses TKIP (Temporal Key Integrity Protocol) data encryption and WPA2-PSK uses AES (Advanced Encryption Standard) data encryption. Both methods dynamically change the encryption keys making them nearly impossible to circumvent. Enter a word or group of printable characters in the Password Phrase box. These characters *are* case sensitive. **Note**: Not all wireless adapter configuration utilities support WPA-PSK and WPA2-PSK. Furthermore, client software is required on the client. Windows XP Service Pack 2 and Windows XP Service Pack 1 with WPA patch do include the client software that supports WPA. However, the wireless adapter hardware and driver must also support WPA.

Balancing performance factors (throughput, latency, battery consumption, and equipment compatibility) against the value of information on your network, select an appropriate security level. As a minimum, NETGEAR recommends using WEP with Shared Key authentication.

Configuring Security in the Advanced Wireless Settings Menu

To configure security in the Advanced Wireless Settings menu:

1. From the main menu of the browser interface, under Advanced, click Wireless Settings. The Advanced Wireless Settings menu appears.

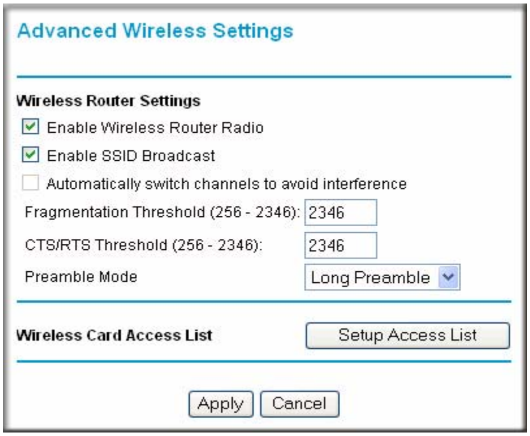


Figure 3-3

The security-related wireless settings are described below. For details on the configuration of the general wireless settings, see “Configuring Wireless Settings” on page 2-10.

- Enable Wireless Router Radio
  If you disable the wireless router radio, wireless devices cannot connect to the WNR834B. If you will not be using your wireless network for a period of time, you can deselect this checkbox and disable all wireless connectivity.
- Enable SSID Broadcast
  Deselect this checkbox to disable broadcast of the SSID, so that only devices that know the correct SSID can connect. Disabling SSID broadcast nullifies the wireless network ‘discovery’ feature of some products such as Windows XP.
- Wireless Card Access List
  When a Wireless Card Access List is configured and enabled, the WNR834B checks the MAC address of any wireless device attempting a connection, and only allows connections to computers identified on the trusted computers list. For instructions on configuring the Wireless Card Access List, see “Restricting Wireless Access by MAC Address” on page 3-12.

Information to Gather Before Changing Basic Wireless Settings

Before customizing your wireless settings, print this form and record the following information. If you are working with an existing wireless network, the person who set up or is responsible for the network will be able to provide this information. Otherwise, you must choose the settings for your wireless network. Either way, record the settings for your wireless network in the spaces below.

- **Wireless Network Name (SSID)*:*** ______________________________ The SSID identifies the wireless network. You can use up to 32 alphanumeric characters. The SSID *is* case sensitive. The SSID in the wireless adapter card must match the SSID of the wireless router. In some configuration utilities (such as in Windows XP), the term “wireless network name” is used instead of SSID.
- If **WEP Authentication** is used, circle one: **Open System**, **Shared Key, or Auto**.

> **Note:** If you select Shared Key, the other devices in the network will not connect unless they are also set to Shared Key and are configured with the correct key.

– **WEP Encryption Key Size**. Choose one: **64-bit** or **128-bit**. Again, the encryption key size must be the same for the wireless adapters and the wireless router.

– **Data Encryption (WEP) Keys**. There are two methods for creating WEP data encryption keys. Whichever method you use, record the key values in the spaces below.

- **Passphrase Method**. ______________________________ These characters *are* case sensitive. Enter a word or group of printable characters and click Generate Keys. Not all wireless devices support the passphrase method.
- **Manual Method**. These values *are not* case sensitive. For 64-bit WEP, enter 10 hexadecimal digits (any combination of 0–9 or a–f). For 128-bit WEP, enter 26 hexadecimal digits.

Key 1: ___________________________________

Key 2: ___________________________________

Key 3: ___________________________________

Key 4: ___________________________________

- If **WPA-PSK or WPA2-PSK Authentication** is used:
  - **Passphrase**: ______________________________ These characters *are* case sensitive. Enter a word or group of printable characters. When you use WPA-PSK, the other devices in the network will not connect unless they are also set to WPA-PSK and are configured with the correct Passphrase. Similarly, when you use WPA2-PSK, the other devices in the network will not connect unless they are aslo set to WPA2-PSK and are configured with the correct Passphrase.

Use the procedures described in the following sections to configure the WNR834B. Store this information in a safe place.

Configuring WEP Wireless Security

To configure WEP data encryption, follow these steps:

Note: If you use a wireless computer to configure WEP settings, you will be disconnected when you click Apply. You must then either configure your wireless adapter to match the wireless router WEP settings or access the wireless router from a wired computer to make any further changes.

1. From the main menu of the browser interface, under Setup, click Wireless Settings.
2. From the Security Options menu, select WEP. The WEP options display.

3. Select the Authentication Type and Encryption strength.

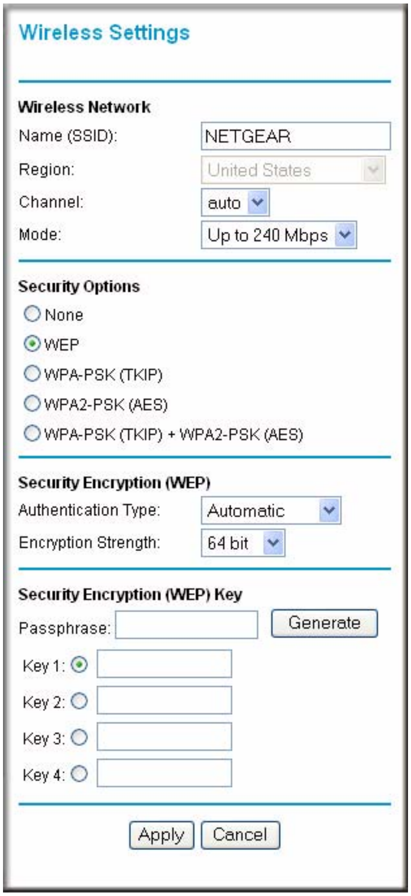


Figure 3-4

4. You can manually or automatically program the four data encryption keys. These values must be identical on all computers and Access Points in your network.
   - **Automatic**. In the Passphrase box, enter a word or group of printable characters and click Generate. The passphrase is case sensitive. For example, NETGEAR is not the same as nETgear. The four key boxes are automatically populated with key values.
   - **Manual**. Enter ten hexadecimal digits (any combination of 0–9, a–f, or A–F). These entries are not case sensitive. For example, AA is the same as aa.
     Select which of the four keys to activate.

See “Wireless Communications” in Appendix B for a full explanation of each of these options, as defined by the IEEE 802.11 wireless communication standard.

5. Click Apply to save your settings.

Configuring WPA-PSK or WPA2-PSK Wireless Security

➡	**Note:** Not all wireless adapters support WPA. Furthermore, client software is also required. Windows XP with Service Pack 2 does include WPA support. Nevertheless, the wireless adapter hardware and driver must also support WPA. For instructions on configuring wireless computers or PDAs (Personal Digital Assistants) for WPA-PSK security, consult the documentation for the product you are using.

To configure WPA-PSK or WPA2-PSK, follow these steps:

1. In the Setup section of the main menu, click Wireless Settings

2. Select one of the WPA-PSK or WPA2-PSK options for the Security Type. The third option (WPA-PSK [TKIP] + WP2-PSK [AES]) is the most flexible, since it allows clients using either WPA-PSK or WPA2-PSK.

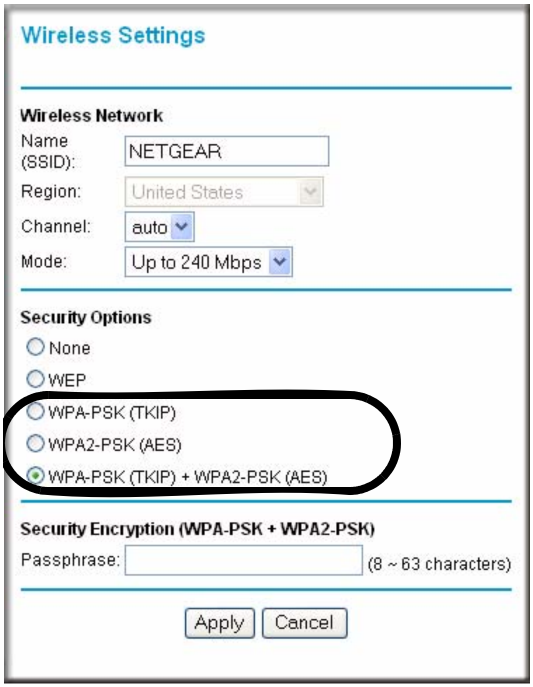


Figure 3-5

3. In the Passphrase box, enter a word or group of 8-63 printable characters. The passphrase is case sensitive.

4. Click Apply to save your settings.

Restricting Wireless Access by MAC Address

By enabling a wireless card access control list, you can restrict access to only trusted computers so that unknown computers cannot wirelessly connect to the WNR834B.

The Wireless Card Access List displays a list of wireless computers that you will allow to connect to the router based on their MAC addresses. These wireless computers must also have the correct SSID and wireless security settings to access the wireless router.

The MAC address is a network device's unique twelve-character physical address, containing the hexadecimal characters 0–9 or A–F only, and separated by colons (for example, `00:09:AB:CD:EF:01`). It can usually be found on the bottom of the wireless card or network interface device. If you do not have access to the physical label, you can display the MAC address using the network configuration utilities of the computer. In WindowsXP, for example, typing the **ipconfig/all** command in an MSDOS Command Prompt window will display the MAC address as Physical Address. You may also find the MAC addresses in the router's Attached Devices menu.

To restrict access based on MAC addresses, follow these steps:

1. In the Advanced section of the main menu, click Wireless Settings

2. From the Wireless Settings menu, click Setup Access List to display the Wireless Card Access List.

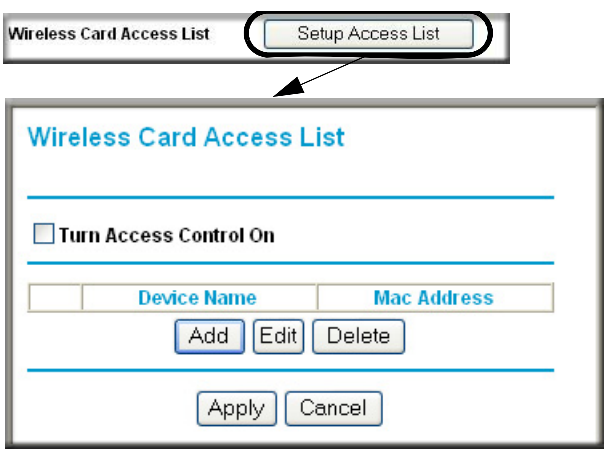


Figure 3-6

3. Click Add to add a wireless device to the wireless access control list. The Wireless Card Access Setup dialog opens and displays a list of currently active wireless cards and their Ethernet MAC addresses.

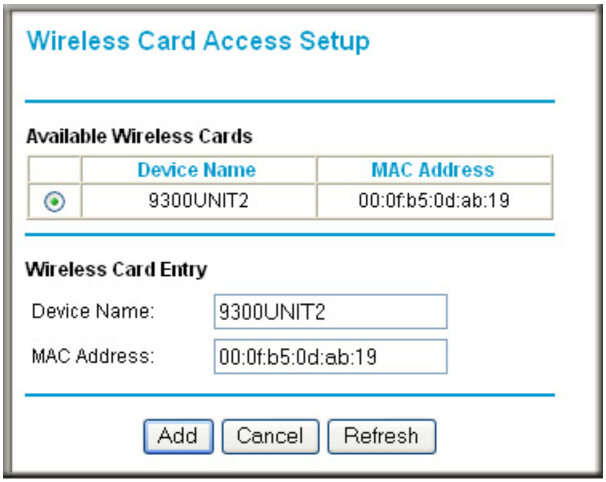


Figure 3-7

4. If the desired computer appears in the Available Wireless Cards list, you can click the radio button of that computer to capture its MAC address; otherwise, you can manually enter a name and the MAC address of the authorized computer. You can usually find the MAC address on the bottom of the wireless device.

	Tip: You can copy and paste the MAC addresses from the router's Attached Devices menu into the MAC Address box of this menu. To do this, configure each wireless computer to obtain a wireless link to the router. The computer should then appear in the Attached Devices menu.

5. Click Add to add this wireless device to the Wireless Card Access List. The screen changes back to the list screen.

6. Repeat step 3 through step 5 for each additional device you want to add to the list.

7. Select the checkbox to Turn Access Control On...

	Note: When configuring the router from a wireless computer whose MAC address is not in the Trusted PC list, if you select Turn Access Control On, you will lose your wireless connection when you click Apply. You must then access the wireless router from a wired computer or from a wireless computer which is on the access control list to make any further changes.

8. Click Apply to save your Wireless Card Access List settings.

Now, only devices on this list are allowed to wirelessly connect to the WNR834B.

	Warning: MAC address filtering adds an obstacle against unwanted access to your network by the general public. However, because your trusted MAC addresses appear in your wireless transmissions, an intruder can read them and impersonate them. Do not rely on MAC address filtering alone to secure your network.

Changing the Administrator Password

The default password for the router's Web Configuration Manager is **password**. NETGEAR recommends that you change this password to a more secure password.

	Tip: Before changing the router password, use the router backup utility to save your configuration settings with the default password of **password**. If you save the settings with a new password, and you later forget the new password, you will have to reset the router back to the factory defaults and log in using the default password of **password**. This means you will have to re-enter all the router configuration settings.

To change the Administrator password:

1. From the main menu of the browser interface, under the Maintenance heading, select Set Password to display the Set Password menu.

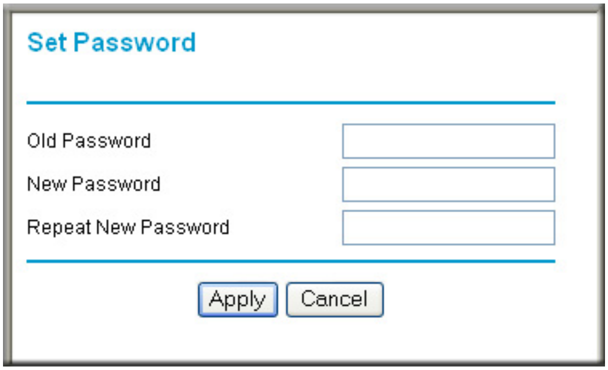


Figure 3-8

2. To change the password, first enter the old password, then enter the new password twice. Click Apply.

Backing Up Your Configuration

The configuration settings of the WNR834B are stored within the router in a configuration file. You can back up (save) this file and retrieve it later. NETGEAR recommends that you save your confguration file after you complete the configuration. In the event of router failure or corruption, or a lost administrator password, you can easily recreate your configuration by restoring the configuration file.

For instructions on saving and restoring your configuration file, see "Managing the Configuration File" on page 7-6.

Tip: Before saving your configuration file, change the administrator password to the default, **password**. Then change it again after you have saved the configuration file. If you save the file with a new password, and you later forget the new password, you will have to reset the router back to the factory defaults and log in using the default password of **password**. This means you will have to re-enter all the router configuration settings.

Understanding Your Firewall

Your RangeMax NEXT Wireless Router WNR834B contains a true firewall to protect your network from attacks and intrusions. A firewall is a device that protects one network from another, while allowing communication between the two. Using a process called stateful packet inspection, the firewall analyzes all inbound and outbound traffic to determine whether or not it will be allowed to pass through.

By default, the firewall allows any outbound traffic and prohibits any inbound traffic except for responses to your outbound traffic. However, you can modify the firewall's rules to achieve the following behavior:

- Blocking sites
  Block access from your network to certain Web locations based on Web addresses and Web address keywords. This feature is described in "Blocking Access to Internet Sites" on page 4-1.
- Blocking services
  Block the use of certain Internet services by specific computers on your network. This feature is described in "Blocking Access to Internet Services" on page 4-3.
- Scheduled blocking
  Block sites and services according to a daily schedule. This feature is described in "Scheduling Blocking" on page 4-5.
- Allow inbound access to your server
  To allow inbound access to resources on your local network (for example, a Web server or remote desktop program), you can open the needed services by configuring port forwarding as described in "Allowing Inbound Connections To Your Network" on page 6-1.
- Allow certain games and applications to function properly
  Some games and applications need to allow additional inbound traffic in order to function. Port triggering can dynamically allow additional service connections, as described in "Allowing Inbound Connections To Your Network" on page 6-1. Another feature to solve application conflicts with the firewall is Universal Plug and Play (UPnP), described in "Using Universal Plug and Play" on page 6-12.

Chapter 4
Restricting Access From Your Network

This chapter describes how to use the content filtering and reporting features of the RangeMax NEXT Wireless Router WNR834B to protect your network. You can find these features by clicking on the Content Filtering heading in the main menu of the browser interface.

This chapter includes:

Content Filtering Overview

The RangeMax NEXT Wireless Router WNR834B provides you with Web content filtering options, plus browser activity reporting and instant alerts via email. Parents and network administrators can establish restricted access policies based on time of day, Web addresses and Web address keywords. You can also block Internet access by applications and services, such as chat or games.

To configure these features of your router, click on the subheadings under the Content Filtering heading in the main menu of the browser interface. This chapter describes the subheadings.

Blocking Access to Internet Sites

The WNR834B router allows you to restrict access based on Web addresses and Web address keywords. Up to 255 entries are supported in the Keyword list.

Keyword application examples:

— If the keyword **XXX** is specified, the URL *www.badstuff.com/xxx.html* is blocked.

— If the keyword .com is specified, only Web sites with other domain suffixes (such as .edu, .org, or .gov) can be viewed.

To block access to Internet sites:

- From the main menu of the browser interface, under Content Filtering, click Block Sites.

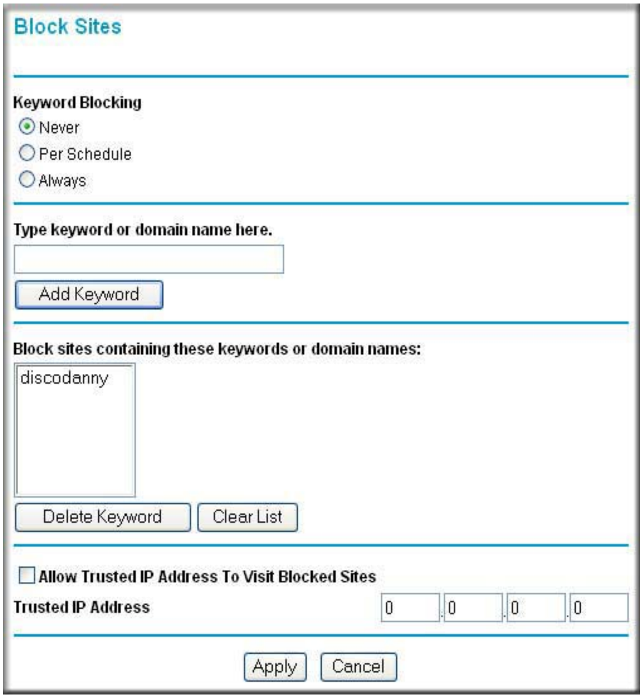


Figure 4-1

— To enable keyword blocking, select either Per Schedule or Always, then click Apply. To block by schedule, be sure to specify a time period in the Schedule menu. For scheduling, see "Scheduling Blocking" on page 4-5.

— To add a keyword or domain, type it in the Keyword box, click Add Keyword, then click Apply.

— To delete a keyword or domain, select it from the list, click Delete Keyword, then click Apply.

— To block all Internet browsing access during a scheduled period, enter a dot (**.**) as the keyword and set the schedule in the Schedule menu.

You may specify one Trusted User, which is a computer that is exempt from blocking and logging. Since the Trusted User is identified by IP address, you should configure that computer with a fixed IP address.

— To specify a Trusted User, enter that computer's IP address in the Trusted User box and click Apply.

Blocking Access to Internet Services

The WNR834B router allows you to block the use of certain Internet services by computers on your network. This is called service blocking or port filtering. Services are functions performed by server computers at the request of client computers. For example, Web servers serve Web pages, time servers serve time and date information, and game hosts serve data about other players' moves. When a computer on your network sends a request for service to a server computer on the Internet, the requested service is identified by a service or port number. This number appears as the destination port number in the transmitted IP packets. For example, a packet that is sent with destination port number 80 is an HTTP (Web server) request.

To block access to Internet Services:

- From the main menu of the browser interface, under Content Filtering, click Block Services.

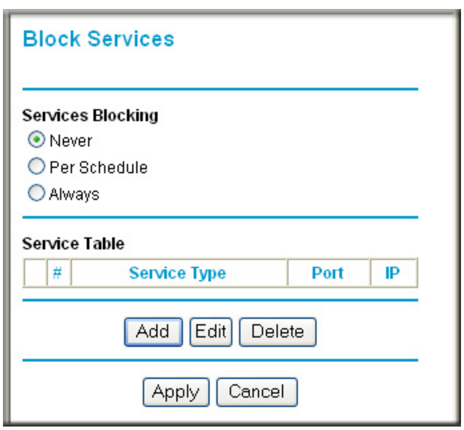


Figure 4-2

— To enable service blocking, select either Per Schedule or Always, then click Apply. To block by schedule, be sure to specify a time period in the Schedule menu. For scheduling, see "Scheduling Blocking" on page 4-5.

— To specify a service for blocking, click Add. The Block Services Setup menu appears.

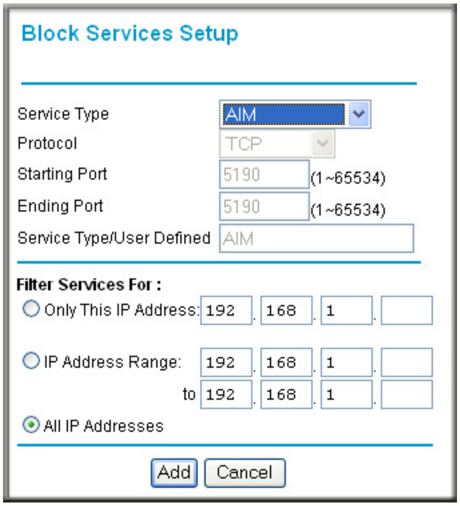


Figure 4-3

— From the Service Type list, select the application or service to be allowed or blocked. The list already displays several common services, but you are not limited to these choices. To add any additional services or applications that do not already appear, select User Defined.

Configuring a User Defined Service

To define a service, first you must determine which port number or range of numbers is used by the application. The service port numbers for many common protocols are defined by the Internet Engineering Task Force (IETF) and published in RFC1700, "Assigned Numbers." Service numbers for other applications are typically chosen from the range 1024 to 65535 by the authors of the application. Port number information can often be determined by contacting the publisher of the application, by asking user groups or newsgroups, or by searching.

— Enter the Starting Port and Ending Port numbers. If the application uses a single port number, enter that number in both boxes.

— If you know that the application uses either TCP or UDP, select the appropriate protocol. If you are not sure, select Both.

Blocking Services by IP Address Range

Under the heading Filter Services For, you can block the specified service for a single computer, a range of computers (having consecutive IP addresses), or all computers on your network.

Scheduling Blocking

The WNR834B router allows you to specify when blocking is enforced. To schedule blocking:

- From the main menu of the browser interface, under Content Filtering, click Schedule.:

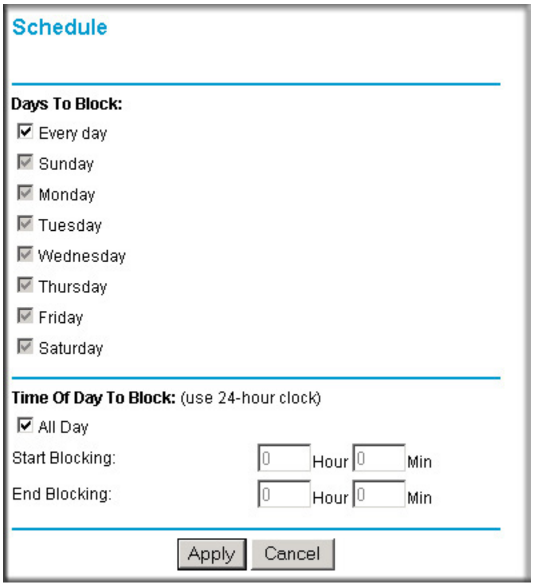


Figure 4-4

Configure the schedule for blocking keywords and services.

- Days to Block
  Select days to block by checking the appropriate boxes. Select Every Day to select the checkboxes for all days. Click Apply.
- Time of Day to Block
  Select a start and end time in 24-hour format. Select All Day for 24-hour blocking. Click Apply.

Be sure to select your Time Zone in the Email menu as described in “Setting the Time” on page 4-8.

Viewing Logs of Web Access or Attempted Web Access

The log is a detailed record of the Web sites you have accessed or attempted to access. Up to 128 entries are stored in the log. Log entries only appear when keyword blocking is enabled, and no log entries are made for the Trusted User.

- From the main menu of the browser interface, under Content Filtering, click Logs.

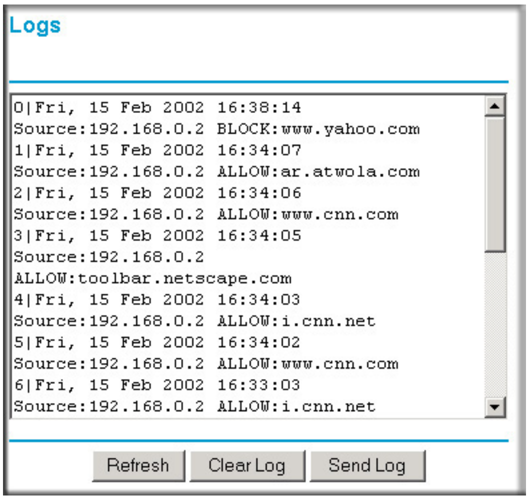


Figure 4-5

Table 4-1 describes the log entries.

Table 4-1. Log entry descriptions

Field	Description
Date and Time	The date and time the log entry was recorded.
Source IP	The IP address of the initiating device for this log entry.
Target address	The name or IP address of the Web site or newsgroup visited or attempted to access.
Action	Whether the access was blocked or allowed.

Table 4-2 describes the log action buttons.

Table 4-2. Log action buttons

Field	Description
Refresh	Click this button to refresh the log screen.
Clear Log	Click this button to clear the log entries.
Send Log	Click this button to email the log immediately.

Configuring Email Alert and Web Access Log Notifications

In order to receive logs and alerts by email, you must provide your email account information. To configure email alert and web access log notifications:

- From the main menu of the browser interface, under Content Filtering, click Email.

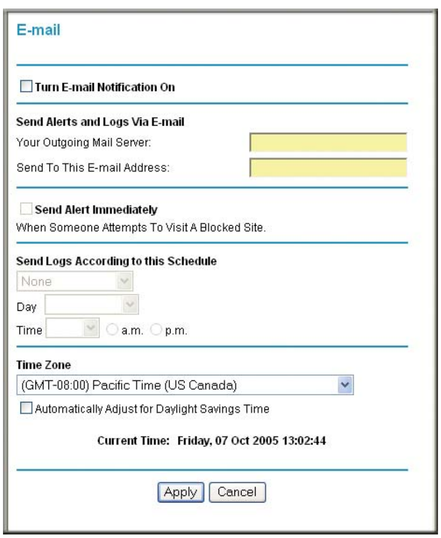


Figure 4-6

— Turn email notification on
Select this checkbox to receive email logs and alerts from the router.

- Your outgoing mail server
  Enter the name of your ISP's outgoing (SMTP) mail server (such as *mail.myISP.com*). You may be able to find this information in the configuration menu of your email program. If you leave this box blank, log and alert messages will not be sent via email.
- Send to this email address
  Enter the email address to which logs and alerts are sent. This email address will also be used as the From address. If you leave this box blank, log and alert messages will not be sent via email.

You can specify that logs are automatically sent by email with these options:

- Send alert immediately
  Select this checkbox for immediate notification of attempted access to a blocked site or service.
- Send logs according to this schedule
  Specifies how often to send the logs: Hourly, Daily, Weekly, or When Full.
  - Day for sending log
    Specifies which day of the week to send the log. Relevant when the log is sent weekly or daily.
  - Time for sending log
    Specifies the time of day to send the log. Relevant when the log is sent daily or weekly.

  If you select the Weekly, Daily or Hourly options and the log fills up before the specified period, the log is automatically emailed to the specified email address. After the log is sent, the log is cleared from the router's memory. If the router cannot email the log file, the log buffer may fill up. In this case, the router overwrites the log and discards its contents.

So that the log entries are properly time-stamped and sent at the correct time, be sure to set the time as described in the next section.

Setting the Time

The WNR834B router uses the Network Time Protocol (NTP) to obtain the current time and date from one of several Network Time Servers on the Internet. In order to localize the time for your log entries, you must specify your Time Zone:

- Time Zone
  Select your local time zone. This setting is used for the blocking schedule and for time-stamping log entries.

- Automatically adjust for Daylight Savings Time
  Select this checkbox if your region supports daylight savings time. The router will automatically adjust the time at the start and end of the Daylight Savings Time period.

Chapter 5
Customizing Your Network Settings

This chapter describes how to configure advanced networking features of the RangeMax NEXT Wireless Router WNR834B, including LAN, WAN, and routing settings.

It describes:

- Using the LAN IP Setup Options
- Using a Dynamic DNS Service
- Configuring the WAN Setup Options
- Configuring Static Routes

Using the LAN IP Setup Options

The LAN IP Setup menu allows configuration of LAN IP services such as Dynamic Host Configuration Protocol (DHCP) and Routing Information Protocol (RIP).

To configure LAN IP Settings:

- From the main menu of the browser interface, under Advanced, click LAN IP Setup to view the LAN IP Setup menu.

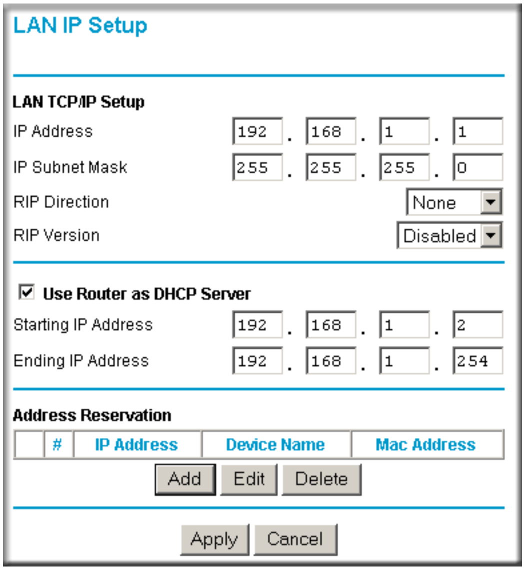


Figure 5-1

Configuring LAN TCP/IP Setup Parameters

The router is shipped preconfigured to use private IP addresses on the LAN side and to act as a DHCP server. The router's default LAN IP configuration is:

- LAN IP address: `192.168.1.1`
- Subnet mask: `255.255.255.0`

These addresses are part of the designated private address range for use in private networks, and should be suitable for most applications. If your network has a requirement to use a different IP addressing scheme, you can make those changes in this menu.

The LAN IP parameters are:

- IP Address
  The LAN IP address of the router.
- IP Subnet Mask
  The LAN Subnet Mask of the router. Combined with the IP address, the IP Subnet Mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or router.

- RIP Direction
  RIP allows a router to exchange routing information with other routers. The RIP Direction selection controls how the router sends and receives RIP packets. Both is the default.
  — When set to Both or Out Only, the router broadcasts its routing table periodically.
  — When set to Both or In Only, the router incorporates the RIP information that it receives.
  — When set to None, the router does not send any RIP packets and ignores any RIP packets received.
- RIP Version
  This controls the format and the broadcasting method of the RIP packets sent by the router. (It recognizes both formats when receiving.) The default setting is RIP-1.
  — RIP-1 is universally supported. RIP-1 is usually adequate unless you have an unusual network setup.
  — RIP-2 carries more information. RIP-2B uses subnet broadcasting.

Note: If you change the LAN IP address of the router while connected through the browser, you will be disconnected. You must then open a new connection to the new IP address and log in again.

Using the Router as a DHCP server

By default, the router functions as a DHCP server, allowing it to assign IP, DNS server, and default gateway addresses to all computers connected to the router's LAN. The assigned default gateway address is the LAN address of the router. The router assigns IP addresses to the attached computers from a pool of addresses specified in this menu. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN.

For most applications, the default DHCP and TCP/IP settings of the router are satisfactory. See “Internet Networking and TCP/IP Addressing” in Appendix B for an explanation of DHCP and information about how to assign IP addresses for your network.

Specify the pool of IP addresses to be assigned by setting the Starting IP Address and Ending IP Address. These addresses should be part of the same IP address subnet as the router’s LAN IP address. Using the default addressing scheme, you should define a range between `192.168.1.2` and `192.168.1.254`, although you may wish to save part of the range for devices with fixed addresses.

The router delivers the following parameters to any LAN device that requests DHCP:

- An IP Address from the range you have defined

- Subnet Mask
- Gateway IP Address (the router’s LAN IP address)
- Primary DNS Server (if you entered a Primary DNS address in the Basic Settings menu; otherwise, the router’s LAN IP address)
- Secondary DNS Server (if you entered a Secondary DNS address in the Basic Settings menu)

To use another device on your network as the DHCP server, or to manually configure the network settings of all of your computers, deselect Use Router as DHCP Server. Otherwise, leave it selected. If you deselect this service and no other DHCP server is available on your network, you will need to set your computers’ IP addresses manually or they will not be able to access the router.

Using Address Reservation

When you specify a reserved IP address for a computer on the LAN, that computer will always receive the same IP address each time it accesses the router’s DHCP server. Reserved IP addresses should be assigned to computers or servers that require permanent IP settings.

To reserve an IP address:

1. Click Add.

2. In the IP Address box, type the IP address to assign to the computer or server. (choose an IP address from the router’s LAN subnet, such as `192.168.1.x`)

3. Type the MAC Address of the computer or server.

> **Tip:** If the computer is already present on your network, you can copy its MAC address from the Attached Devices menu and paste it here.

4. Click Apply to enter the reserved address into the table.

> **Note:** The reserved address is not assigned until the next time the computer contacts the router's DHCP server. Reboot the computer or access its IP configuration and force a DHCP release and renew.

To edit or delete a reserved address entry:

1. Click the button next to the reserved address you want to edit or delete.

2. Click Edit or Delete.

Using a Dynamic DNS Service

If your Internet Service Provider (ISP) gives you a permanently assigned IP address, you can register a domain name and have that name linked with your IP address by public Domain Name Servers (DNS). However, if your Internet account uses a dynamically assigned IP address, you do not know in advance what your IP address will be, and the address can change frequently. In this case, you can use a commercial dynamic DNS service, which will allow you to register your domain to their IP address, and will forward traffic directed at your domain to your frequently changing IP address.

Note: If your ISP assigns a private WAN IP address (such as `192.168.x.x` or `10.x.x.x`), the dynamic DNS service will not work because private addresses are not routed on the Internet.

Your router contains a client that can connect to the dynamic DNS service provided by DynDNS.org. You must first visit their website at *www.dyndns.org* and obtain an account and host name, which you will configure in the router. Then, whenever your ISP-assigned IP address changes, your router will automatically contact the dynamic DNS service provider, log in to your account, and register your new IP address. If your host name is *hostname*, you will be able to reach your router at *hostname.dyndns.org*.

From the main menu of the browser interface, under Advanced, click on Dynamic DNS to view the Dynamic DNS menu.

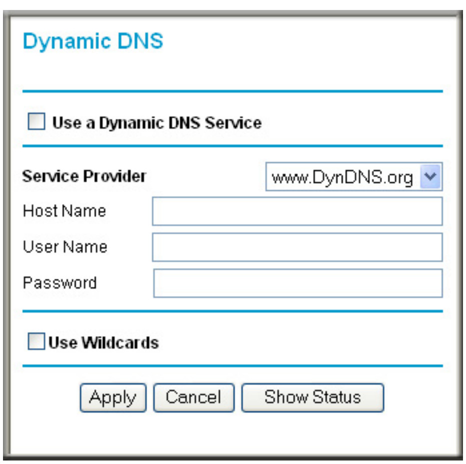


Figure 5-2

To configure Dynamic DNS:

1. Register for an account with one of the dynamic DNS service providers whose names appear in the Select Service Provider box. For example, for DynDNS.org, go to *www.dyndns.org*.
2. Select the checkbox for Use a Dynamic DNS Service.
3. Select the name of your dynamic DNS Service Provider.
4. Type the Host Name (or domain name) that your dynamic DNS service provider gave you.
5. Type the User Name for your dynamic DNS account.
   This is the name you use to log in to your account, not your host name.
6. Type the Password (or key) for your dynamic DNS account.
7. If your dynamic DNS provider allows the use of wildcards in resolving your URL, you can select the Use Wildcards checkbox to activate this feature.
   For example, the wildcard feature will cause **.yourhost.dyndns.org* to be aliased to the same IP address as *yourhost.dyndns.org*.
8. Click Apply to save your configuration.

Configuring the WAN Setup Options

The WAN Setup options let you configure a DMZ (De-Militarized Zone) server, change the Maximum Transmit Unit (MTU) size, and enable the wireless router to respond to a ping on the WAN port. From the main menu of the browser interface, under Advanced, click WAN Setup to view the WAN Setup menu.

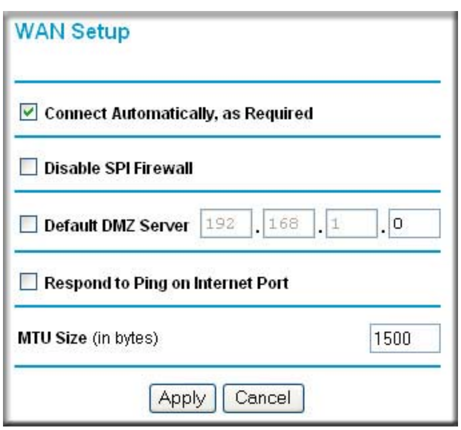


Figure 5-3

Connecting Automatically, as Required

Normally, this option should be selected so that an Internet connection will be made automatically after each timeout, whenever Internet-bound traffic is detected. This feature provides connection on demand and is potentially cost-saving in regions where Internet services charge by the minute, as in some areas of Europe.

If this feature is disabled, you must connect manually, using the Connection Status button on the Router Status screen. The manual connection will stay up continuously without timeouts.

Disabling the SPI Firewall

The Stateful Packet Inspection (SPI) Firewall protects your network and computers against attacks and intrusions. A stateful packet firewall carefully inspects incoming traffic packets, looking for known exploits such as malformed, oversized, or out-of-sequence packets. The firewall should only be disabled in special circumstances, such as when troubleshooting application issues.

Setting Up a Default DMZ Server

The default DMZ server feature is helpful when using some online games and videoconferencing applications that are incompatible with Network Address Translation (NAT). The router is programmed to recognize some of these applications and to work properly with them, but there are other applications that may not function well. In some cases, one local computer can run the application properly if that computer's IP address is entered as the default DMZ server.

> **Warning:** DMZ servers pose a security risk. A computer designated as the default DMZ server loses much of the protection of the firewall, and is exposed to exploits from the Internet. If compromised, the DMZ server computer can be used to attack other computers on your network.

Incoming traffic from the Internet is normally discarded by the router unless the traffic is a response to one of your local computers or a service that you have configured in the Port Forwarding/Port Triggering menu. Instead of discarding this traffic, you can have it forwarded to one computer on your network. This computer is called the Default DMZ Server.

The WAN Setup menu lets you configure a Default DMZ Server.

To assign a computer or server to be a Default DMZ server:

1. In the main menu, under Advanced, click WAN Setup.

2. Under Default DMZ Server, type the last digit of the IP address for that computer. To remove the default DMZ server, enter zero.
3. Select the checkbox for Default DMZ Server and click Apply.

Responding to a Ping on the Internet WAN Port

If you want the router to respond to a 'ping' from the Internet, select the checkbox for Respond to Ping on Internet WAN Port. This should only be used as a diagnostic tool, since it allows your router to be discovered by Internet scanners. Do not select this checkbox unless you have a specific reason to do so, such as when troubleshooting your connection.

Setting the MTU Size

The normal MTU value for most Ethernet networks is 1500 bytes, 1492 bytes for PPPoE connections, or 1436 for PPTP connections. For some ISPs, you may need to reduce the MTU, but this is rarely required and should not be done unless you are sure it is necessary for your ISP connection. For more information, see "Changing the MTU" on page 6-14.

To change the MTU size:

1. Under MTU Size, enter a new size between 64 and 1500.
2. Click Apply to save the new configuration.

Configuring Static Routes

Static routes provide additional routing information to your router. Under normal circumstances, the router has adequate routing information after it has been configured for Internet access, and you do not need to configure additional static routes. You must configure static routes only for unusual cases such as multiple routers or multiple IP subnets located on your network.

From the main menu of the browser interface, under Advanced, click Static Routes to view the Static Routes menu.

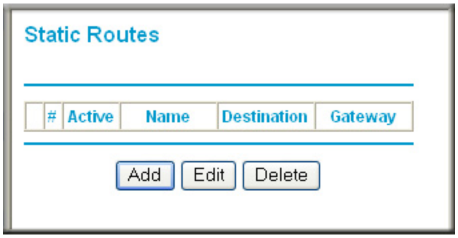


Figure 5-4

To add or edit a static route:

1. Click Add to open the Add Static Routes menu.

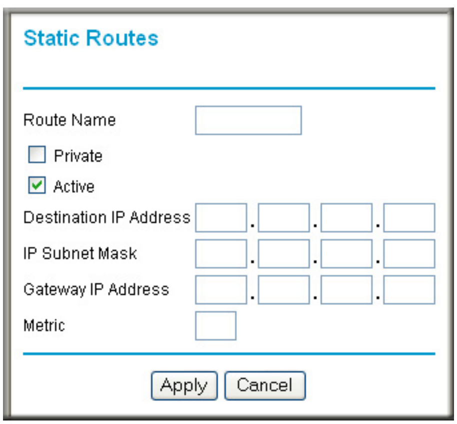


Figure 5-5

2. In the Route Name box, type a name for this static route.
   (This is for identification purposes only.)
3. Select the Private checkbox if you want to limit access to the LAN only.
   If Private, the static route will not be reported in RIP.
4. Select the Active checkbox to make this route effective.
5. Type the Destination IP Address of the final destination.
6. Type the IP Subnet Mask for this destination.
   If the destination is a single host, type `255.255.255.255`.

7. Type the Gateway IP Address, which must be a router on the same LAN segment as the WNR834B.
8. Type a number between 1 and 15 as the metric value.
   This represents the number of routers between your network and the destination. Usually, a setting of 2 or 3 works, but if this is a direct connection, set it to 1.
9. Click Apply to have the static route entered into the table.

As an example of when a static route is needed, consider the following case:

- Your primary Internet access is through a cable modem to an ISP.
- You have an ISDN router on your home network for connecting to the company where you are employed. This router's address on your LAN is `192.168.1.100`.
- Your company's network address is `134.177.0.0`.

When you first configured your router, two implicit static routes were created. A default route was created with your ISP as the gateway, and a second static route was created to your local network for all `192.168.1.x` addresses. With this configuration, if you attempt to access a device on the `134.177.0.0` network, your router will forward your request to the ISP. The ISP forwards your request to the company where you are employed, and the request will likely be denied by the company's firewall.

In this case you must define a static route, telling your router that `134.177.0.0` should be accessed through the ISDN router at `192.168.1.100`. The static route would look like Figure 5-5 on page 5-9.

In this example:

- The Destination IP Address and IP Subnet Mask fields specify that this static route applies to all `134.177.x.x` addresses.
- The Gateway IP Address fields specifies that all traffic for these addresses should be forwarded to the ISDN router at `192.168.1.100`.
- A metric value of 1 will work since the ISDN router is on the LAN.
- Private is selected only as a precautionary security measure in case RIP is activated.

Chapter 6
Fine-Tuning Your Network

This chapter describes how to modify the configuration of the RangeMax NEXT Wireless Router WNR834B to allow specific applications to access the Internet or to be accessed from the Internet, and how to make adjustments to enhance your network's performance.

This chapter includes:

Allowing Inbound Connections To Your Network

By default, the WNR834B router blocks any inbound traffic from the Internet to your computers except for replies to your outbound traffic. However, you may need to create exceptions to this rule for the following purposes:

- To allow remote computers on the Internet to access a server on your local network.
- To allow certain applications and games to work properly when their replies are not recognized by your router.

Your router provides two features for creating these exceptions: Port Forwarding and Port Triggering. This section explains how a normal outbound connection works, followed by two examples explaining how Port Forwarding and Port Triggering operate and how they differ.

How Your Computer Communicates With A Remote Computer Through Your Router

When a computer on your network needs to access a computer on the Internet, your computer sends your router a message containing source and destination address and process information. Before forwarding your message to the remote computer, your router must modify the source information and must create and track the communication session so that replies can be routed back to your computer.

Here is an example of normal outbound traffic and the resulting inbound responses:

a. You open Internet Explorer, beginning a browser session on your computer. Invisible to you, your operating system assigns a service number (port number) to every communication process running on your computer. In this example, let's say Windows assigns port number 5678 to this browser session.

b. You ask your browser to get a Web page from the Web server at *www.example.com.* Your computer composes a Web page request message with the following address and port information:

- The source address is your computer's IP address.
- The source port number is 5678, the browser session.
- The destination address is the IP address of *www.example.com*, which your computer finds by asking a DNS server.
- The destination port number is 80, the standard port number for a Web server process.

Your computer then sends this request message to your router.

c. Your router creates an entry in its internal session table describing this communication session between your computer and the Web server at *www.example.com*. Before sending the Web page request message to *www.example.com*, your router stores the original information and then modifies the source information in the request message, performing Network Address Translation (NAT):

- The source address is replaced with your router's public IP address.
  This is necessary because your computer uses a private IP address that is not globally unique and cannot be used on the Internet.
- The source port number is changed to a number chosen by the router, such as 33333.
  This is necessary because two computers could independently be using the same session number.

Your router then sends this request message through the Internet to the Web server at *www.example.com*.

d. The Web server at *www.example.com* composes a return message with the requested Web page data. The return message contains the following address and port information:

— The source address is the IP address of *www.example.com*.

— The source port number is 80, the standard port number for a Web server process.

— The destination address is the public IP address of your router.

— The destination port number is 33333.

The Web server then sends this reply message to your router.

e. Upon receiving the incoming message, your router checks its session table to determine whether there is an active session for port number 33333. Finding an active session, the router then modifies the message, restoring the original address information replaced by NAT. The message now contains the following address and port information:

— The source address is the IP address of *www.example.com*.

— The source port number is 80, the standard port number for a Web server process.

— The destination address is your computer’s IP address.

— The destination port number is 5678, the browser session that made the initial request.

Your router then sends this reply message to your computer, which displays the Web page from *www.example.com*.

f. When you finish your browser session, your router eventually senses a period of inactivity in the communications. Your router then removes the session information from its session table, and incoming traffic is no longer accepted on port number 33333.

How Port Triggering Changes the Communication Process

In the preceding example, requests are sent to a remote computer by your router from a particular service port number and replies from the remote computer to your router are directed to that port number. If the remote server sends a reply back to a different port number, your router will not recognize it and will discard it. However, some application servers (such as FTP and IRC servers) send replies back to multiple port numbers. Using the Port Triggering function of your router, you can tell the router to open additional incoming ports when a particular outgoing port originates a session.

An example is Internet Relay Chat (IRC). Your computer connects to an IRC server at destination port 6667. The IRC server not only responds to your originating source port, but also sends an “identify” message to your computer on port 113. Using Port Triggering, you can tell the router, “When you initiate a session with destination port 6667, you must also allow incoming traffic on port 113 to reach the originating computer.” Using steps similar to the preceding example, the following sequence shows the effects of the Port Triggering rule you have defined:

a. You open an IRC client program, beginning a chat session on your computer.

b. Your IRC client composes a request message to an IRC server using a destination port number of 6667, the standard port number for an IRC server process. Your computer then sends this request message to your router.

c. Your router creates an entry in its internal session table describing this communication session between your computer and the IRC server. Your router stores the original information, performs Network Address Translation (NAT) on the source address and port, and sends this request message through the Internet to the IRC server.

d. Noting your Port Triggering rule, and having observed the destination port number of 6667, your router creates an additional session entry to send any incoming port 113 traffic to your computer.

e. The IRC server sends a return message to your router using the NAT-assigned source port (as in the previous example, let's say port 33333) as the destination port. The IRC server also sends an "identify" message to your router with destination port 113.

f. Upon receiving the incoming message to destination port 33333, your router checks its session table to determine whether there is an active session for port number 33333. Finding an active session, the router restores the original address information replaced by NAT and sends this reply message to your computer.

g. Upon receiving the incoming message to destination port 113, your router checks its session table and learns that there is an active session for port 113, associated with your computer. The router replaces the message's destination IP address with your computer's IP address and forwards the message to your computer.

h. When you finish your chat session, your router eventually senses a period of inactivity in the communications. The router then removes the session information from its session table, and incoming traffic is no longer accepted on port numbers 33333 or 113.

To configure Port Triggering, you need to know which inbound ports the application needs. Also, you need to know the outbound port number that will trigger the opening of the inbound ports. This information can usually be determined by contacting the publisher of the application or from user groups or newsgroups..

⇨	**Note:** Only one computer at a time can use the triggered application.

How Port Forwarding Changes the Communication Process

In both of the preceding examples, your computer initiates an application session with a server computer on the Internet. However, you may need to allow a client computer on the Internet to initiate a connection to a server computer on your network. Normally, your router will ignore any inbound traffic that is not a response to your own outbound traffic. You can configure exceptions to this default rule by using the Port Forwarding feature.

A typical application of Port Forwarding can be shown by reversing the client/server relationship from our previous Web server example. In this case, a remote computer's browser needs to access a Web server running on a computer in your local network. Using Port Forwarding, you can tell the router, "When you receive incoming traffic on port 80 (the standard port number for a Web server process), forward it to the local computer at `192.168.1.123`." The following sequence shows the effects of the Port Forwarding rule you have defined:

a. The user of a remote computer opens Internet Explorer and requests a Web page from *www.example.com*, which resolves to the public IP address of your router. The remote computer composes a Web page request message with the following destination information:

— The destination address is the IP address of *www.example.com*, which is the address of your router.

— The destination port number is 80, the standard port number for a Web server process.

The remote computer then sends this request message through the Internet to your router.

b. Your router receives the request message and looks in its rules table for any rules covering the disposition of incoming port 80 traffic. **Your Port Forwarding rule specifies that incoming port 80 traffic should be forwarded to local IP address `192.168.1.123`. Therefore, your router modifies the destination information in the request message:**

— The destination address is replaced with `192.168.1.123`.

Your router then sends this request message to your local network.

c. Your Web server at `192.168.1.123` receives the request and composes a return message with the requested Web page data. Your Web server then sends this reply message to your router.

d. Your router performs Network Address Translation (NAT) on the source IP address, and sends this request message through the Internet to the remote computer, which displays the Web page from *www.example.com*.

To configure Port Forwarding, you need to know which inbound ports the application needs. This information can usually be determined by contacting the publisher of the application or from user groups or newsgroups.

How Port Forwarding Differs From Port Triggering

- Port Triggering can be used by any computer on your network, although only one computer may use it at a time.
- Port Forwarding is configured for a single computer on your network.
- Port Triggering does not need to know the computer's IP address in advance. The IP address will be captured automatically.
- Port Forwarding requires that you specify the computer's IP address during configuration, and the IP address must never change.
- Port Triggering requires specific outbound traffic to open the inbound ports, and the triggered ports will be closed after a period of no activity.
- Port Forwarding is always active and does not need to be triggered.

Configuring Port Forwarding to Local Servers

Using the Port Forwarding feature, you can allow certain types of incoming traffic to reach servers on your local network. For example, you may make a local Web server, FTP server, or game server visible and available to the Internet.

Use the Port Forwarding menu to configure the router to forward specific incoming protocols to computers on your local network. In addition to servers for specific applications, you can also specify a Default DMZ Server to which all other incoming protocols are forwarded. The DMZ Server is configured in the WAN Setup menu as discussed in "Setting Up a Default DMZ Server" on page 5-7.

Before starting, you need to determine which type of service, application or game you will provide, and the local IP address of the computer that will provide the service. Be sure the computer's IP address never changes.



Tip: To ensure that your server computer always has the same IP address, use the reserved IP address feature of your WNR834B router. See "Using Address Reservation" on page 5-4 for instructions on how to use reserved IP addresses.

To configure port forwarding to a local server:

1. From the main menu of the browser interface, under Advanced, click on Port Forwarding /Port Triggering to view the port forwarding menu.

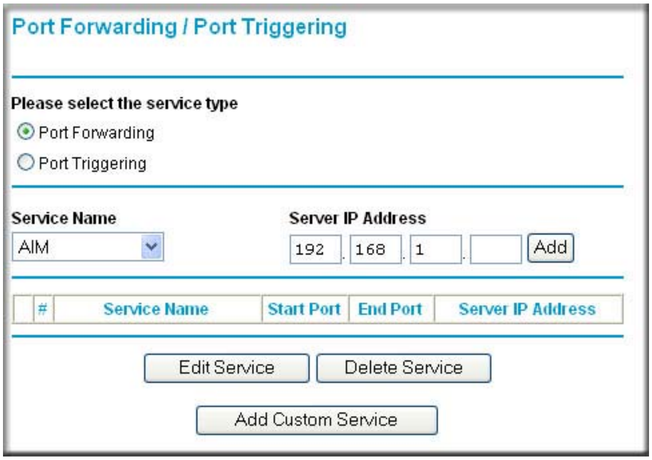


Figure 6-1

2. From the Service Name box, select the service or game that you will host on your network. If the service does not appear in the list, see the following section, "Adding a Custom Service".
3. In the corresponding Server IP Address box, enter the last digit of the IP address of your local computer that will provide this service.
4. Click Add. The service will appear in the list on the menu.

Adding a Custom Service

To define a service, game, or application that does not appear in the Service Name list, you must first determine which port number or range of numbers is used by the application. This information can usually be determined by contacting the publisher of the application or from user groups or newsgroups. When you have the port number information, follow these steps:

1. From the main menu of the browser interface, under Advanced, click Port Forwarding /Port Triggering.

2. Click Add Custom Service.

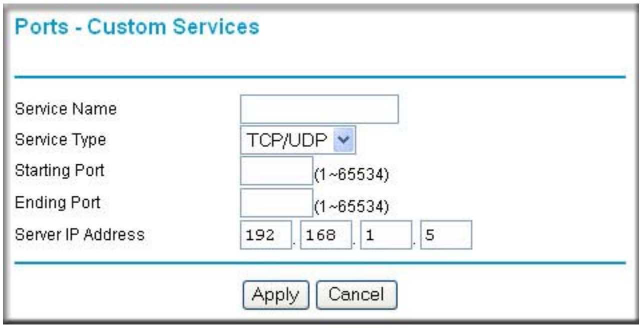


Figure 6-2

3. In the Service Name box, type a descriptive name.
4. In the Service Type box, select the protocol. If you are unsure, select TCP/UDP.
5. In the Starting Port box, type the beginning port number.
   - If the application uses only a single port, type the same port number in the Ending Port box.
   - If the application uses a range of ports, type the ending port number of the range in the Ending Port box.
6. In the Server IP Address box, type the IP address of your local computer that will provide this service.
7. Click Apply. The service will appear in the list in the Port Forwarding /Port Triggering menu.

Editing or Deleting a Port Forwarding Entry

To edit or delete a Port Forwarding entry:

1. In the table, select the button next to the service name.
2. Click Edit Service or Delete Service.

Application Example: Making a Local Web Server Public

If you host a Web server on your local network, you can use Port Forwarding to allow Web requests from anyone on the Internet to reach your Web server.

To make a local Web server public:

1. Assign your Web server either a fixed IP address or a dynamic IP address using DHCP Address Reservation, as explained in "Using Address Reservation" on page 5-4. In this example, your router will always give your Web server an IP address of `192.168.1.33.`
2. Configure the Port Forwarding menu to forward the HTTP service to the local address of your Web server at `192.168.1.33.`
   HTTP (port 80) is the standard protocol for Web servers.
3. (Optional) Register a host name with a Dynamic DNS Service and configure your router to use the name as described in "Using a Dynamic DNS Service" on page 5-5.
   To access your Web server from the Internet, a remote user must know the IP address that has been assigned by your ISP. However, if you use a Dynamic DNS Service, the remote user can reach your server by a user-friendly Internet name, such as *mynetgear.dyndns.org*.

Configuring Port Triggering

Port Triggering is a dynamic extension of Port Forwarding that is useful when:

- More than one local computer needs port forwarding for the same application (but not simultaneously) or
- An application needs to open incoming ports that are different from the outgoing port.

When Port Triggering is enabled, the router monitors outbound traffic looking for a specified outbound "trigger" port. When the router detects outbound traffic on that port, it remembers the IP address of the local computer that sent the data. The router then temporarily opens the specified incoming port or ports, and forwards incoming traffic on the triggered ports to the triggering computer.

While Port Forwarding creates a static mapping of a port number or range to a single local computer, Port Triggering can dynamically open ports to any computer that needs them and can close the ports when they are no longer needed.

Note: If you use applications such as multi-player gaming, peer-to-peer connections, real-time communications such as instant messaging, or remote assistance (a feature in Windows XP), you should also enable Universal Plug and Play (UPnP) according to the instructions in "Using Universal Plug and Play" on page 6-12.

To configure Port Triggering, you need to know which inbound ports the application needs. Also, you need to know the outbound port number that will trigger the opening of the inbound ports. This information can usually be determined by contacting the publisher of the application or from user groups or newsgroups.

To set up Port Triggering:

1. In the main menu, under Advanced, Select Port Forwarding/Port Triggering.
2. Select the Port Triggering radio button. The Port Triggering screen appears.

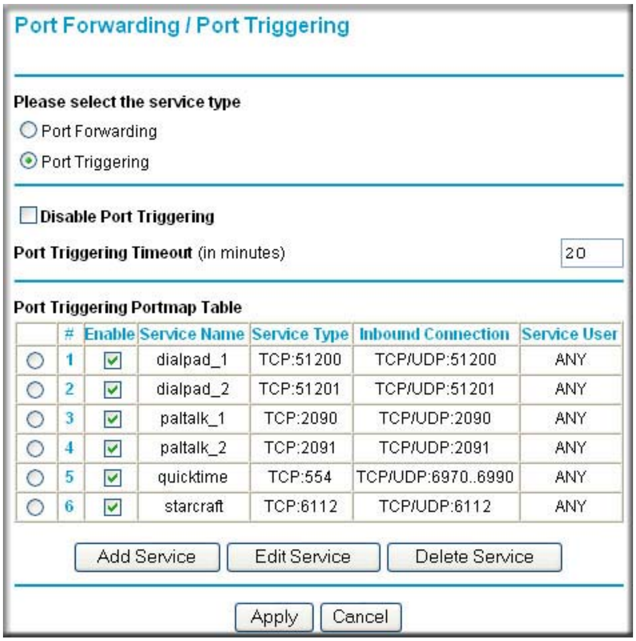


Figure 6-3

3. Deselect the checkbox for Disable Port Triggering.

Note: If the Disable Port Triggering checkbox is selected after configuring port triggering, port triggering is disabled. However, any port triggering configuration information you added to the router is retained even though it will not be used.

4. For Port Triggering Timeout, enter a value up to 9999 minutes. This value controls the inactivity timer for the designated inbound port(s). The inbound port(s) close when the inactivity timer expires. This is required because the router cannot be sure when the application has terminated.

5. Click Add Service.

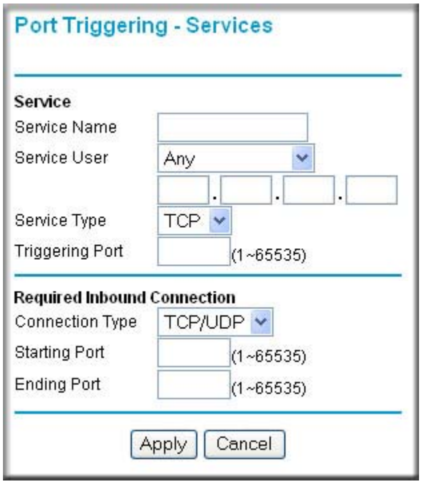


Figure 6-4

6. In the Service Name box, type a descriptive service name.
7. Under Service User, select Any (default) to allow this service to be used by any computer on the Internet. Otherwise, select Single address and enter the IP address of one computer to restrict the service to a particular computer.
8. Select the Service Type, either TCP or UDP or both (TCP/UDP). If you are not sure, select TCP/UDP.
9. In the Triggering Port box, enter the outbound traffic port number that will cause the inbound ports to be opened.
10. Enter the inbound connection port information such as Connection Type, Starting Port, and Ending Port boxes.
11. Click Apply. The service appears in the Port Triggering Portmap Table.

Using Universal Plug and Play

Universal Plug and Play (UPnP) helps devices, such as Internet appliances and computers, to access the network and connect to other devices as needed. UPnP devices can automatically discover the services from other registered UPnP devices on the network.

Note: If you use applications such as multi-player gaming, peer-to-peer connections, real-time communications such as instant messaging, or remote assistance (a feature in Windows XP), you should enable UPnP.

From the main menu of the browser interface, under Advanced, click UPnP. The UPnP menu appears.

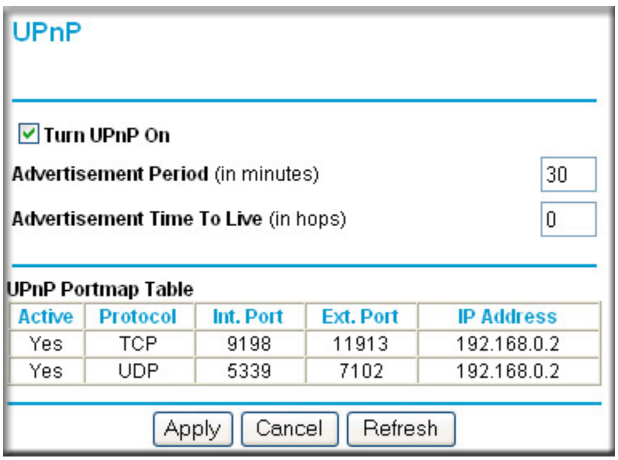


Figure 6-5

The available settings and displays in this menu are:

- Turn UPnP On
  UPnP can be enabled or disabled for automatic device configuration. The default setting for UPnP is disabled. If disabled, the router will not allow any device to automatically control the resources, such as port forwarding (mapping) of the router.

- Advertisement Period
  The Advertisement Period is how often the router will broadcast its UPnP information. This value can range from 1 to 1440 minutes. The default period is 30 minutes. Shorter durations ensure that control points have current device status at the expense of additional network traffic. Longer durations may compromise the freshness of the device status but can significantly reduce network traffic.
- Advertisement Time To Live
  The time to live for the advertisement is measured in hops (steps) for each UPnP packet sent. The time to live hop count is the number of steps a broadcast packet is allowed to propagate for each UPnP advertisement before it disappears. The number of hops can range from 1 to 255. The default value for the advertisement time to live is 4 hops, which should be fine for most home networks. If you notice that some devices are not being updated or reached correctly, then it may be necessary to increase this value.
- UPnP Portmap Table
  The UPnP Portmap Table displays the IP address of each UPnP device that is currently accessing the router and which ports (Internal and External) that device has opened. The UPnP Portmap Table also displays what type of port is open and whether that port is still active for each IP address.

Optimizing Wireless Performance

The speed and operating distance or range of your wireless connection can vary significantly based on the physical placement of the wireless router. You should choose a location for your router that will maximize the network speed.

Note: Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the router. For complete range and performance specifications, please see “Wireless Communications” in Appendix B.

The following list describes how to optimize wireless router performance.

- Identify critical wireless links.
  If your network has several wireless devices, decide which wireless devices need the highest data rate, and locate the router near them. Many wireless products have automatic data-rate fallback, which allows increased distances without losing connectivity. This also means that devices that are further away may be slower. Therefore, the most critical links in your network are those where the traffic is high and the distances are great. Optimize those first.

- Choose placement carefully.
  For best results, place your router:
  - Near the center of the area in which your computers will operate.
  - In an elevated location such as a high shelf where the wirelessly connected computers have line-of-sight access (even if through walls).
- Avoid obstacles to wireless signals.
  - Keep wireless devices at least two feet from large metal fixtures such as file cabinets, refrigerators, pipes, metal ceilings, reinforced concrete, and metal partitions.
  - Keep away from large amounts of water such as fish tanks and water coolers.
- Reduce interference.
  Avoid windows unless communicating between buildings.
  Place wireless devices away from various electromagnetic noise sources, especially those in the 2400–2500 MHz frequency band. Common noise-creating sources are:
  - Computers and fax machines (no closer than one foot)
  - Copying machines, elevators, and cell phones (no closer than 6 feet)
  - Microwave ovens (no closer than 10 feet)
- Choose your settings.
  - Use a scanning utility to determine what other wireless networks are operating nearby, and choose an unused channel.
  - Turn off SSID Broadcast, and change the default SSID. Other nearby devices may automatically try to connect to your network several times a second, which can cause significant performance reduction.

Changing the MTU

The Maximum Transmission Unit (MTU) is the largest data packet a network device transmits. When one network device communicates across the Internet with another, the data packets travel through many devices along the way. If any device in the data path has a lower MTU setting than the other devices, the data packets must be split or “fragmented” to accommodate the one with the smallest MTU.

The best MTU setting for NETGEAR equipment is often just the default value, and changing the value may fix one problem but cause another. Leave MTU unchanged unless:

- You have problems connecting to your ISP, or other Internet service, and either the technical support of the ISP or of NETGEAR recommends changing MTU. These may require an MTU change:
  - A secure Web site that won't open, or only displays part of a Web page
  - Yahoo email
  - MSN
  - America Online's DSL service
- You use VPN and have severe performance problems.
- You used a program to optimize MTU for performance reasons, and now you have connectivity or performance problems..

Note: An incorrect MTU setting can cause Internet communication problems such as the inability to access certain Web sites, frames within Web sites, secure login pages, FTP or POP servers.

If you suspect an MTU problem, a common solution is to change the MTU to 1400. If you are willing to experiment, you can gradually reduce the MTU from the maximum value of 1500 until the problem goes away. Table 6-1 describes common MTU sizes and applications.

Table 6-1. Common MTU Sizes

MTU	Application
1500	The largest Ethernet packet size and the default value. This is the typical setting for non-PPPoE, non-VPN connections, and is the default value for NETGEAR routers, adapters, and switches.
1492	Used in PPPoE environments.
1472	Maximum size to use for pinging. (Larger packets are fragmented.)
1468	Used in some DHCP environments.
1460	Usable by AOL if you don't have large email attachments, for example.
1436	Used in PPTP environments or with VPN.
1400	Maximum size for AOL DSL.
576	Typical value to connect to dial-up ISPs.

To change the MTU size:

1. In the Advanced section of the main menu, click WAN Setup.
2. Under MTU Size, enter a new size between 64 and 1500.

3. Click Apply to save the new configuration.

Optimizing Your Network Bandwidth

As your network grows, it may consist of several segments of different networking technologies, each providing different throughput. In planning your network, you should first consider which devices will have the heaviest traffic flow between them. Examples are:

- A media center in one room streaming high-definition video from a server in another room
- A storage device that is used for backing up your computers

Next, consider the throughput of your network devices. Where possible, make the heaviest-traffic connections using higher-speed technologies, with no lower-speed bottlenecks in the path.

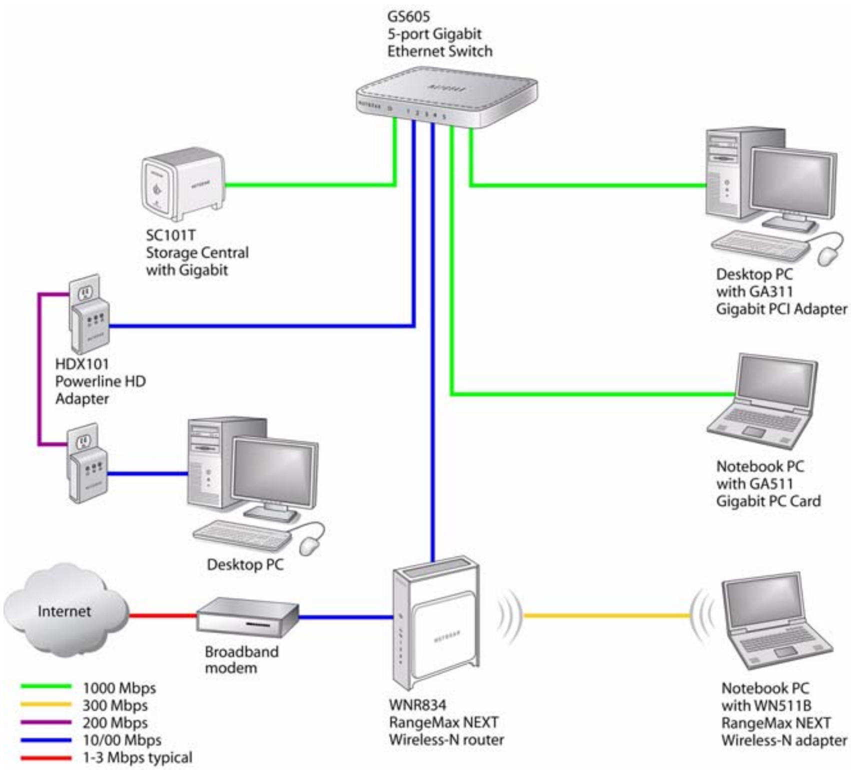


Figure 6-6

Figure 6-6 shows an example network using multiple networking technologies. In this network, the two PCs with gigabit (1000 Mbps) Ethernet adapters have a gigabit connection through the GS605 switch to the storage server. This connection should allow for extremely fast backups or quick access to large files on the server. The PC connected through a pair of Powerline HD adapters is limited to the 200 Mbps speed of the Powerline HD connection. Although any of the links in this example would be sufficient for high-traffic applications such as streaming HD video, the use of older devices such as 10 Mbps Ethernet or 802.11b wireless would create a significant bottleneck.

Overview of Home and Small Office Networking Technologies

Common connection types and their speed and security considerations are:

- **Broadband Internet**
  Your Internet connection speed is determined by your modem type, such as ADSL or cable modem, as well as the connection speed of the sites to which you connect, and general Internet traffic. ADSL and cable modem connections are asymmetrical, meaning they have a lower data rate *to* the Internet (upstream) than *from* the Internet (downstream). Keep in mind that when you connect to someone else who also has an asymmetrical connection, the data rate between your sites is limited by each side's upstream data rate. A typical residential ADSL or cablemodem connection provides a downstream throughput of about one to three megabits per second (Mbps). Newer technologies such as ADSL2+ and Fiber to the Home (FTTH) will increase the connection speed to tens of Mbps.
- **Wireless**
  Your RangeMax NEXT Wireless Router WNR834B provides a wireless data throughput of up to 300 Mbps using technology called Multiple-Input Multiple-Output (MIMO), in which multiple antennas transmit multiple streams of data. The use of multiple antennas also provides excellent range and coverage. With the introduction of the newer WPA and WPA2 encryption and authentication protocols, wireless security is extremely strong.

  To get the best performance, use RangeMax NEXT adapters such as the WN511B for your computers. Although the RangeMax NEXT router is compatible with older 802.11b and 802.11g adapters, the use of these older wireless technologies in your network can result in lower throughput overall (typically less than 10 Mbps for 802.11b and less than 40 Mbps for 802.11g). In addition, many older wireless products do not support the latest security protocols, WPA and WPA2.

- **Powerline**
  For connecting rooms or floors that are blocked by obstructions or are distant vertically, consider networking over your building's AC wiring. NETGEAR's Powerline HD family of products delivers up to 200 Mbps to any outlet, while the older generation XE family of products delivers 14 Mbps or 85 Mbps. Data transmissions are encrypted for security, and you can configure an individual network password to prevent neighbors from connecting.

  The Powerline HD family of products can coexist on the same network with older generation XE family products or HomePlug 1.0 products, but they are not interoperable with these older products.
- **Wired Ethernet**
  As gigabit-speed Ethernet ports (10/100/1000 Mbps) become common on newer computers, wired Ethernet remains a good choice for speed, economy, and security. Gigabit Ethernet can extend up to 100 meters with twisted-pair wiring of CAT-5e or better. A wired connection is not susceptible to interference, and eavesdropping would require a physical connection to your network.

Note: Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, can lower actual data throughput rate.

Assessing Your Speed Requirements

Because your Internet connection is likely to operate at a much lower speed than your local network, faster local networking technologies may not improve your Internet experience. However, many emerging home applications require high data rates. For example:

- Streaming HD video requires 10 to 30 Mbps per stream. Because latency and packet loss can disrupt your video, plan to provide at least twice the capacity you need.
- Streaming MP3 audio requires less than 1 Mbps per stream and does not strain most modern networks. Like video, however, streaming audio is also sensitive to latency and packet loss, so a congested network or a noisy link can cause problems.

- Backing up computers over the network has become popular due to the availability of inexpensive mass storage. Table 6-2 shows the time to transfer one gigabyte (1 GB) of data using various networking technologies.

Table 6-2. Theoretical Transfer Time for 1 Gigabyte

Network Connection	Theoretical Raw Transfer Time
Gigabit Wired Ethernet	8 seconds
RangeMax NEXT Wireless-N	26 seconds
Powerline HD	40 seconds
100 Mbps Wired Ethernet	80 seconds
802.11g wireless	150 seconds
802.11b wireless	700 seconds
10 Mbps Wired Ethernet	800 seconds
Cable Modem (3 Mbps)	2700 seconds
Analog Modem (56 kbps)	144,000 seconds (40 hours)

Chapter 7
Using Network Monitoring Tools

This chapter describes how to use the maintenance features of your RangeMax NEXT Wireless Router WNR834B. These features can be found by clicking on the Maintenance heading in the main menu of the browser interface.

This chapter includes:

- Viewing Wireless Router Status Information
- Viewing a List of Attached Devices
- Managing the Configuration File
- Erasing the Configuration
- Upgrading the Router Software
- Enabling Remote Management Access

Viewing Wireless Router Status Information

To view router status and usage information:

- From the main menu of the browser interface, under Maintenance, select Router Status.

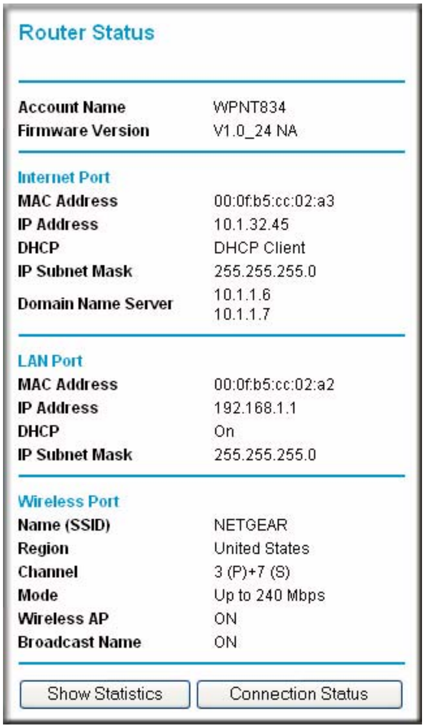


Figure 7-1

Table 7-1 describes the router status fields.

Table 7-1. Wireless Router Status Fields

Field	Description
Account Name	The Host Name assigned to the router.
Firmware Version	The version of the current software installed in the router. This will change if you upgrade your router.

Table 7-1. Wireless Router Status Fields (continued)

Field	Description
Internet Port	These parameters apply to the Internet (WAN) port of the router.
MAC Address	The Media Access Control address. This is the unique physical address being used by the Internet (WAN) port of the router.
IP Address	The IP address being used by the Internet (WAN) port of the router. If no address is shown, or is 0.0.0.0, the router cannot connect to the Internet.
DHCP	If set to None, the router is configured to use a fixed IP address on the WAN. If set to DHCP Client, the router is configured to obtain an IP address dynamically from the ISP.
IP Subnet Mask	The IP Subnet Mask being used by the Internet (WAN) port of the router. For an explanation of subnet masks and subnet addressing, see "Internet Networking and TCP/IP Addressing" in Appendix B.
Domain Name Server	The Domain Name Server addresses being used by the router. A Domain Name Server translates human-language URLs such as *www.netgear.com* into IP addresses.
LAN Port	These parameters apply to the Local (LAN) port of the router.
MAC Address	The Media Access Control address. This is the unique physical address being used by the LAN port of the router.
IP Address	The IP address being used by the Local (LAN) port of the router. The default is `192.168.1.1`.
DHCP	Identifies whether the router's built-in DHCP server is active for the LAN attached devices.
IP Subnet Mask	The IP Subnet Mask being used by the Local (LAN) port of the router. The default is `255.255.255.0`.
Wireless Port	These parameters apply to the Wireless port of the router.
Name (SSID)	The wireless network name (SSID) being used by the wireless port of the router. The default is NETGEAR.
Region	The geographic region where the router is being used. It may be illegal to use the wireless features of the router in some parts of the world.
Channel	Identifies the channel of the wireless port being used. See "Wireless Communications" in Appendix B for the frequencies used on each channel. In "Up to 240 Mbps" mode, there are two channels: a primary channel (P) and a secondary channel (S).
Mode	Indicates the wireless communication mode: 802.11g and 802.11b, 802.11g only, up to 126 Mbps, or up to 240 Mbps.

Table 7-1. Wireless Router Status Fields (continued)

Field	Description
Wireless AP	Indicates whether the radio feature of the router is enabled. If not enabled, the Wireless LED on the front panel will be off.
Broadcast Name	Indicates whether the router is broadcasting its SSID.

Click Connection Status to display the connection status.

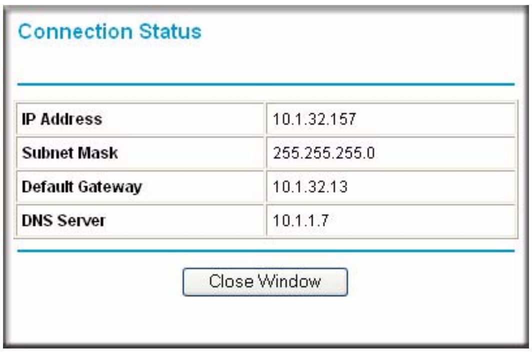


Figure 7-2

Table 7-2 describes the connection status settings...

Table 7-2. Connection Status Items

Item	Description
IP Address	The WAN (Internet) IP Address assigned to the router.
Subnet Mask	The WAN (Internet) Subnet Mask assigned to the router.
Default Gateway	The WAN (Internet) default gateway the router communicates with.
DNS Server	The IP address of the Domain Name Service server that provides translation of network names to IP addresses.

Click Show Statistics to display router usage statistics.

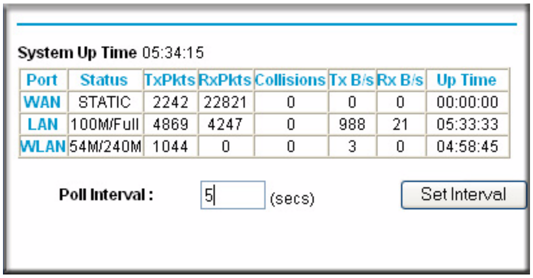


Figure 7-3

Table 7-3 describes the router statistics.

Table 7-3. Router Statistics Items

Item	Description
System Up Time	The elapsed time since the router was last restarted.
Port	The statistics for the WAN (Internet) and LAN (local) ports. For each port, the screen displays:
Status	The link status of the port.
TxPkts	The number of packets transmitted on this port since reset or manual clear.
RxPkts	The number of packets received on this port since reset or manual clear.
Collisions	The number of collisions on this port since reset or manual clear.
Tx B/s	The current transmission (outbound) bandwidth used on the WAN and LAN ports.
Rx B/s	The current reception (inbound) bandwidth used on the WAN and LAN ports.
Up Time	The time elapsed since this port acquired the link.
Poll Interval	The intervals at which the statistics are updated in this window.
Set Interval	To change the polling frequency, enter a time and click Set Interval.

Viewing a List of Attached Devices

The Attached Devices table contains a table of all IP devices that the router has discovered on the local network. From the main menu of the browser interface, under the Maintenance heading, select Attached Devices to view the table.

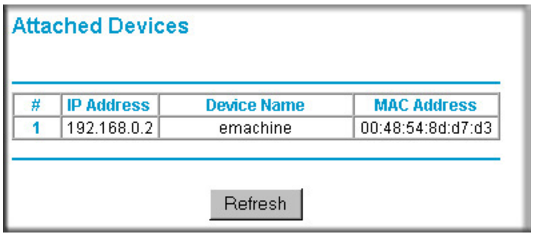


Figure 7-4

For each device, the table shows the IP address, NetBIOS Host Name or Device Name (if available), and the Ethernet MAC address. To force the router to look for attached devices, click Refresh.

> **Note:** If the router is rebooted, the table data is lost until the router rediscovers the devices.

Managing the Configuration File

The configuration settings of the WNR834B are stored within the router in a configuration file. You can back up (save) this file to your computer, restore it, or reset it to the factory default settings.

From the main menu of the browser interface, under the Maintenance heading, select Backup Settings**.**

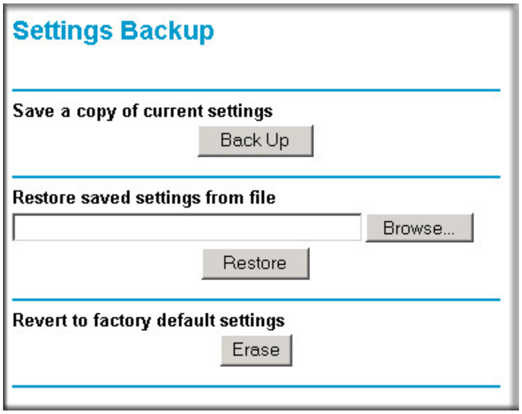


Figure 7-5

The following sections describe the three available options.

Backing Up and Restoring the Configuration

The Restore and Backup options in the Settings Backup menu let you save and retrieve a file containing your router's configuration settings.

To save your settings, click Back Up. Your browser will extract the configuration file from the router and prompt you for a location on your computer to store the file. You can give the file a meaningful name at this time, such as COMCAST.CFG.

Tip: Before saving your configuration file, change the administrator password to the default, **password**. Then change it again after you have saved the configuration file. In the event that you forget the password, you will need to reset the configuration to factory defaults.

To restore your settings from a saved configuration file, enter the full path to the file on your computer or click Browse to browse to the file. When you have located it, click Restore to send the file to the router. The router will then reboot automatically.

Warning: Do not interrupt the reboot process.

Erasing the Configuration

Under some circumstances (for example, if you move the router to a different network or if you have forgotten the password) you may want to erase the configuration and restore the factory default settings. After an erase, the router's username is **admin**, the password is **password**, the LAN IP address is `192.168.1.1` (or *www.routerlogin.net*), and the router's DHCP server is enabled.

To erase the configuration, click the Erase button.

To restore the factory default configuration settings without knowing the login password or IP address, you must use the Default Reset button on the rear panel of the router. See "Problems with Date and Time" on page 8-9.

Upgrading the Router Software

Tip: To ensure that you are always using the latest firmware, enable the Firmware Upgrade Assistant feature so that the router will automatically detect a new version of the firmware on the Internet and alert you to its availability.

This screen appears at login unless you check Do Not Display This Message Again and click Yes.

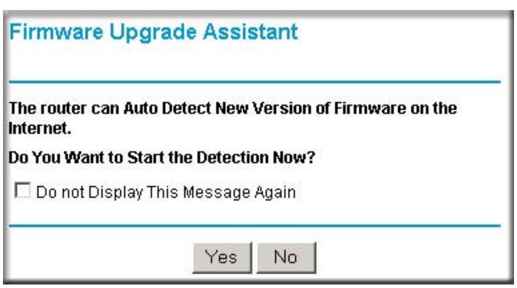


Figure 7-6

Tip: Before upgrading the router software, use the router Backup menu to save your configuration settings. A router upgrade might revert the router settings back to the factory defaults. If so, after completing the upgrade, you can restore your settings from the backup.

The routing software of the WNR834B router is stored in FLASH memory, and can be upgraded as new software is released by NETGEAR. You can download upgrade files from the NETGEAR Web site. If the upgrade file is compressed (.ZIP file), you must first extract the file before sending it to the router. You can use your browser to send the upgrade file to the router.

> **Note:** The Web browser used to upload new firmware into the WNR834B router must support HTTP uploads. NETGEAR recommends using Internet Explorer 5.1, Firefox 1.0.5, or later versions.

From the main menu of the browser interface, under the Maintenance heading, select Router Upgrade to display the upgrade menu.

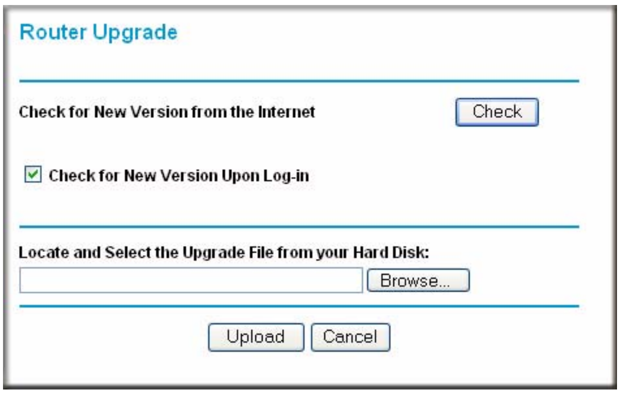


Figure 7-7

To upload new firmware:

1. Click Check to download and unzip (if the download file is a .ZIP file) the new software file from NETGEAR.
2. Click Browse and browse to the location of the new software file.
3. Click Upload.

> **Warning:** When uploading software to the WNR834B router, *do not* interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it could corrupt the software.

When the upload is complete, your router will automatically restart. The upgrade process typically takes about one minute. Read the new software release notes to determine whether you must reconfigure the router after upgrading.

Enabling Remote Management Access

Using the Remote Management feature, you can allow a user on the Internet to configure, upgrade, and check the status of your WNR834B router. From the main menu of the browser interface, under the Advanced heading, select Remote Management.

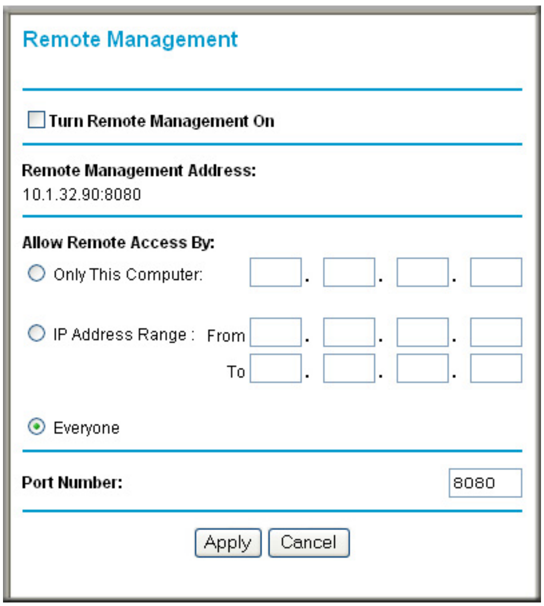


Figure 7-8

	Note: Be sure to change the router's default configuration password to a very secure password. The ideal password should contain no dictionary words from any language, and should be a mixture of letters (both upper and lower case), numbers, and symbols. Your password can be up to 30 characters.

To configure your router for remote management:

1. Select the checkbox to Turn Remote Management On.

2. Under the heading of Allow Remote Access By, specify what external IP addresses will be allowed to access the router's remote management.

> **Note:** For enhanced security, restrict access to as few external IP addresses as practical.

   a. To allow access from any IP address on the Internet, select Everyone.
   b. To allow access from a range of IP addresses on the Internet, select IP address range. Enter a beginning and ending IP address to define the allowed range.
   c. To allow access from a single IP address on the Internet, select Only This Computer. Enter the IP address that will be allowed access.

3. Specify the Port Number for accessing the management interface.

   Normal Web browser access uses the standard HTTP service port 80. For greater security, enter a custom port number for the remote management Web interface. Choose a number between 1024 and 65535, but do not use the number of any common service port. The default is 8080, which is a common alternate for HTTP.

4. Click Apply to have your changes take effect.

> **Note:** When accessing your router from the Internet, type your router's WAN IP address into your browser's address (in Internet Explorer) or location box, followed by a colon (:) and the custom port number. For example, if your external address is `134.177.0.123` and you use port number 8080, then enter **`http://134.177.0.123:8080`** in your browser.

Chapter 8
Troubleshooting

This chapter provides information about troubleshooting your RangeMax NEXT Wireless Router WNR834B. After each problem description, instructions are provided to help you diagnose and solve the problem. As a first step, please review the Quick Tips.

> **Tip:** NETGEAR provides helpful articles, documentation, and the latest software updates at *http://kbserver.netgear.com/products/WNR834B.asp*.

This chapter includes:

- Troubleshooting Quick Tips
- Troubleshooting Basic Functions
- Troubleshooting the Web Configuration Interface
- Troubleshooting the Internet Connection
- Troubleshooting a Network Using a Ping Utility
- Problems with Date and Time
- Solving Wireless Connection Problems
- Restoring the Default Configuration and Password

Troubleshooting Quick Tips

This section describes tips for troubleshooting some common problems:

Be sure to restart your network in this sequence.

1. Turn off *and* unplug the modem.
2. Turn off the wireless router and computers.
3. Plug in the modem and turn it on. Wait 2 minutes.
4. Turn on the wireless router and wait 1 minute.

5. Turn on the computers.

Make sure the Ethernet cables are securely plugged in.

- The Internet status light on the wireless router will be lit if the Ethernet cable connecting the wireless router and the modem is plugged in securely and the modem and wireless router are turned on.
- For each powered on computer connected to the wireless router by an Ethernet cable, the corresponding numbered router LAN port light will be lit.

Make sure the wireless settings in the computer and router match exactly.

- For a wirelessly connected computer, the Wireless Network Name (SSID) and WEP or WPA security settings of the router and wireless computer must match exactly.
- If you have enabled the wireless router to restrict wireless access by MAC address, you must add the wireless computer's MAC address to the router's wireless card access list.

Make sure the network settings of the computer are correct.

- Wired and wirelessly connected computers *must* have network (IP) addresses on the same network as the router. The simplest way to do this is to configure each computer to obtain an IP address automatically using DHCP. Please see "Preparing a Computer for Network Access" in Appendix B or the documentation that came with your computer.
- Some cable modem service providers require you to use the MAC address of the computer initially registered on the account. Your wireless router can capture and use that MAC address, as described in "Configuring Your Internet Connection Using the Smart Setup Wizard" on page 2-5.

Check the test light to verify correct router operation.

If the Test light does not turn off within 2 minutes after turning the router on, reset the router according to the instructions in "Problems with Date and Time" on page 8-9.

Troubleshooting Basic Functions

After you turn on power to the router, the following sequence of events should occur:

1. When power is first applied, verify that the Power light  is on.

2. After approximately 10 seconds, verify that:

a. The power light is solidly on.

b. The Internet light is lit.

c. A numbered LAN port light is lit for any local port that is connected to a computer. This indicates that a link has been established to the connected device.

If any of the above conditions does not occur, see the appropriate following section.

The power light is not on or is blinking.

If the Power and other lights are off when your router is turned on:

- Make sure that the power cord is properly connected to your router and that the power adapter is properly connected to a functioning power outlet.
- Check that you are using the 12V DC 1A power adapter that NETGEAR supplied for this product.
- If the Power light alternately blinks green and amber every second, the router software is corrupted. This can happen if a firmware upgrade is interrupted, or if the router detects a problem with the firmware. For recovery instructions, contact technical support at *www.netgear.com/support*.

If the error persists, you have a hardware problem and should contact technical support at *www.netgear.com/support*.

The lights never turn off,

When the router is turned on, the lights turns on for about 10 seconds and then turn off. If all the lights stay on, there is a fault within the router.

If all lights are still on one minute after power up:

- Cycle the power to see if the router recovers.
- Clear the router's configuration to factory defaults as explained in "Problems with Date and Time" on page 8-9.

If the error persists, you might have a hardware problem and should contact technical support at *www.netgear.com/support*.

The LAN or WAN port lights are not lit.

If either the LAN port lights or Internet light do not light when the Ethernet connection is made, check the following:

- Make sure that the Ethernet cable connections are secure at the router and at the modem or computer.
- Make sure that power is turned on to the connected modem or computer.
- Be sure you are using the correct cable:
  - When connecting the router's Internet port to a cable or DSL modem, use the cable that was supplied with the cable or DSL modem. This cable could be a standard straight-through Ethernet cable or an Ethernet crossover cable.

The Wireless light is not lit.

If the Wireless light does not come on, verify that the wireless feature is turned on according to the instructions in "Configuring Security in the Advanced Wireless Settings Menu" on page 3-6.

Troubleshooting the Web Configuration Interface

If you are unable to access the router's Web Configuration interface from a computer on your local network, check the following:

- If you are connecting from a wireless computer, try connecting from a wired computer.
- Check the Ethernet connection between the wired computer and the router as described in "Troubleshooting Basic Functions" on page 8-2.
- Make sure your computer's IP address is on the same subnet as the router. For instructions, see "Preparing a Computer for Network Access" in Appendix B to configure your computer.

Note: If your computer's IP address is shown as `169.254.x.x`: Windows and Mac OS will generate and assign an IP address if the computer cannot reach a DHCP server. These auto-generated addresses are in subnet `169.254.x.x`. If your IP address is in this range, check the connection from the computer to the router and reboot your computer.

- Make sure your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click Refresh to be sure the Java applet is loaded.
- Try quitting the browser and launching it again, or try a different browser.
- Make sure you are using the correct login information. The factory default login name is **admin** and the password is **password**. Make sure that CAPS LOCK is off when entering this information.

If the router does not save changes you have made in the Web Configuration Interface, check the following:

- When entering configuration settings, be sure to click Apply before moving to another menu or tab, or your changes could be lost.
- Click Refresh or Reload in the Web browser. The changes may have occurred, but the Web browser may be caching the old configuration.

Troubleshooting the Internet Connection

If you can access your router but you are unable to access the Internet, you should first determine whether the router is able to obtain an IP address from your Internet Service Provider (ISP). Unless your ISP provides a static IP address, your router must request an IP address from the ISP. You can determine whether the request was successful using the Web Configuration Manager.

To check the WAN IP address:

1. Launch your browser and select an external site such as *www.netgear.com.*
2. Access the main menu of the router's configuration at *http://www.routerlogin.net*.
3. Under the Maintenance heading, select Router Status.
4. Check that an IP address is shown for the WAN Port.
   If `0.0.0.0` is shown, your router has not obtained an IP address from your ISP.

If your router is unable to obtain an IP address from the ISP, you may need to force your cable or DSL modem to recognize your new router by restarting your network, as described in "Be sure to restart your network in this sequence. " on page 8-1.

If your router is still unable to obtain an IP address from the ISP, the problem may be one of the following:

- Your ISP may require a login program.
  Ask your ISP whether they require PPP over Ethernet (PPPoE) or some other type of login.
- If your ISP requires a login, you may have incorrectly set the login name and password.
- Your ISP may check for your computer's host name.
  Assign the computer Host Name of your ISP account as the Account Name in the Basic Settings menu.
- Your ISP only allows one Ethernet MAC address to connect to Internet and might check for your computer's MAC address. In this case:

  Inform your ISP that you have bought a new network device, and ask them to use the router's MAC address.

  OR

  Configure your router to spoof your computer's MAC address. This procedure is explained in "Configuring Your Internet Connection Using the Smart Setup Wizard" on page 2-5.

If your router can obtain an IP address, but your computer is unable to load any Web pages from the Internet:

- Your computer may not recognize any DNS server addresses.

  A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically, your ISP will provide the addresses of one or two DNS servers for your use. If you entered a DNS address during the router's configuration, reboot your computer and verify the DNS address as described in "Preparing a Computer for Network Access" in Appendix B. You can also configure your computer manually with DNS addresses, as explained in your operating system documentation.

- Your computer may not have the router configured as its TCP/IP gateway.

  If your computer obtains its information from the router by DHCP, reboot the computer and verify the gateway address as described in "Preparing a Computer for Network Access" in Appendix B.

- You may be running login software that is no longer needed.

  If your ISP provided a program to log you in to the Internet (such as WinPoET), you no longer need to run that software after installing your router. You may need to go to the Internet Explorer Tools menu, Internet Options, Connections tab and select "Never dial a connection."

Troubleshooting a Network Using a Ping Utility

Most network devices and routers contain a ping utility that sends an echo request packet to the designated device. The device then responds with an echo reply. Troubleshooting a network is made very easy by using the ping utility in your computer or workstation.

Testing the LAN Path to Your Router

You can ping the router from your computer to verify that the LAN path to your router is set up correctly.

To ping the router from a running Windows PC:

1. From the Windows toolbar, click Start, and then select Run.
2. In the field provided, type `ping` followed by the IP address of the router, as in this example:
   `ping www.routerlogin.net`
3. Click **OK**.

   You should see a message like this one:
   `Pinging <IP address > with 32 bytes of data`

   If the path is working, you see this message:

```
Reply from < IP address >: bytes=32 time=NN ms TTL=xxx
```

If the path is not working, you see this message:

```
Request timed out
```

If the path is not functioning correctly, you could have one of the following problems:

- Wrong physical connections
  - — For a wired connection, make sure the numbered LAN port light is on for the port to which you are connected. If the light is off, follow the instructions in "The LAN or WAN port lights are not lit." on page 8-3.
  - — Check that the corresponding Link lights are on for your network interface card. If your router and computer are connected to a separate Ethernet switch, make sure the link lights are on for the switch ports that are connected to your computer and router.
- Wrong network configuration
  - — Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your computer.
  - — Verify that the IP address for your router and your computer are correct and that the addresses are on the same subnet.

Testing the Path from Your Computer to a Remote Device

After verifying that the LAN path works correctly, test the path from your computer to a remote device. From the Windows run menu, type:

PING -n 10 *<IP address>*

where <*IP address*> is the IP address of a remote device such as your ISP's DNS server.

If the path is functioning correctly, replies like those shown in the previous section are displayed. If you do not receive replies:

- — Check that your computer has the IP address of your router listed as the default gateway. If the IP configuration of your computer is assigned by DHCP, this information will not be visible in your computer's Network Control Panel. Verify that the IP address of the router is listed as the default gateway as described in "Preparing a Computer for Network Access" in Appendix B.
- — Check to see that the network address of your computer (the portion of the IP address specified by the subnet mask) is different from the network address of the remote device.
- — Check that your cable or DSL modem is connected and functioning.

— If your ISP assigned a host name to your computer, enter that host name as the Account Name in the Basic Settings menu.

— Your ISP could be rejecting the Ethernet MAC addresses of all but one of your computers. Many broadband ISPs restrict access by only allowing traffic from the MAC address of your broadband modem, but some ISPs additionally restrict access to the MAC address of a single computer connected to that modem. If this is the case, you must configure your router to “clone” or “spoof” the MAC address from the authorized computer. For more information, see “Configuring Your Internet Connection Using the Smart Setup Wizard” on page 2-5.

Problems with Date and Time

The Email menu in the Content Filtering section displays the current date and time of day. The WNR834B router uses the Network Time Protocol (NTP) to obtain the current time from one of several Network Time Servers on the Internet. Each entry in the log is stamped with the date and time of day. Problems with the date and time function can include:

- Date shown is January 1, 2000.
  Cause: The router has not yet successfully reached a Network Time Server. Check that your Internet access settings are configured correctly. If you have just completed configuring the router, wait at least five minutes and check the date and time again.
- Time is off by one hour.
  Cause: The router does not adjust for Daylight Savings Time. In the Email menu, check the box marked “Adjust for Daylight Savings Time”.

Solving Wireless Connection Problems

The first steps in solving wireless connection problems are:

1. Using your wireless card’s setup utility program, make sure your wireless card can find your wireless router.
2. Configure and test with the simplest wireless connection possible, and then add security.

The topics in this section describe these steps.

Using Your Wireless Card Setup Program

When you install a NETGEAR wireless card in your computer, a Smart Wizard utility program is installed that can provide helpful information about your wireless network. You can find this program in your Windows program menu or as an icon in your system tray. Other wireless card manufacturers may include a similar program.

If you have no specific wireless card setup program installed, you can use the basic setup utility in Windows by following these steps:

1. Open the Windows Control Panel and select Network Connections.
2. Under the LAN section, double-click Wireless Network Connection.

Use the setup program to scan for available wireless networks. Look for a Network Name (SSID) of NETGEAR or your custom SSID if you have changed it. If your wireless network does not appear, check these conditions:

- Is your router's wireless radio enabled? See "Configuring Security in the Advanced Wireless Settings Menu" on page 3-6.
- Is your router's SSID Broadcast enabled? See "Configuring Security in the Advanced Wireless Settings Menu" on page 3-6.
- Is your router set to a wireless standard that is not supported by your wireless card? Check the Mode setting in "Configuring Wireless Settings" on page 2-10.

If your wireless network appears, but the signal strength is weak, check these conditions:

- Is your router too far from your computer, or too close? Place your computer near the router, but at least six feet away and see whether the signal strength improves.
- Is your wireless signal obstructed by objects between the router and your computer? See "Optimizing Wireless Performance" on page 6-13.

If your wireless network appears and has good signal strength, configure your wireless card and router for the simplest possible connection as described in the next section.

Setting Up and Testing Basic Wireless Connectivity

> **Note:** If you use a wireless computer to change wireless settings, you may be disconnected when you click Apply. Reconfigure your wireless adapter to match the new settings or access the wireless router from a wired computer to make any further changes.

Follow the instructions below to set up and test basic wireless connectivity. Once you have established basic wireless connectivity, you can enable security settings appropriate to your needs.

1. In the main menu of the WNR834B router, under the heading Setup, click Wireless Settings**.**

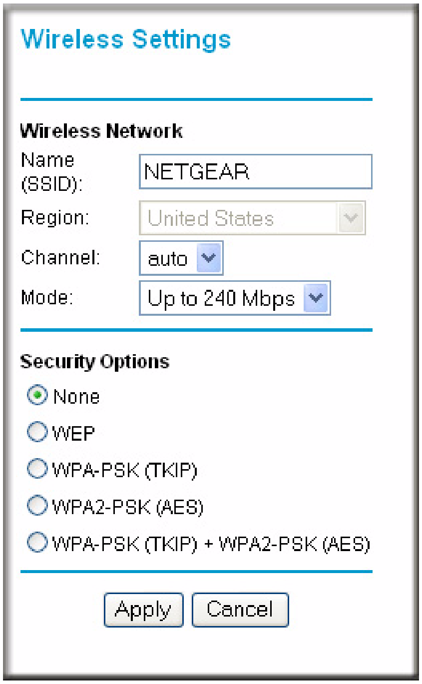


Figure 8-1

2. For the wireless network name (SSID), use the default name or choose a suitable descriptive name. In the SSID box, you can enter a value of up to 32 alphanumeric characters. The default SSID is NETGEAR.

> **Note:** The SSID is case sensitive; NETGEAR is not the same as nETgear. Also, the SSID of any wireless access adapters must match the SSID you configure in the RangeMax NEXT Wireless Router WNR834B. If they do not match, you will not get a wireless connection to the WNR834B.

3. Set the Region. Select the region in which the wireless interface will operate.

4. Set the Channel. The default channel is Auto.

This field determines which operating frequency is used. It should not be necessary to change the wireless channel unless you notice interference problems with another nearby wireless router or access point. Select a channel that is not being used by any other wireless networks within several hundred feet of your router. For more information on the wireless channel frequencies, see "Wireless Communications" in Appendix B.

5. Set the Mode to g and b.
6. For Security Options, select None.
7. Click Apply to save your changes.

> **Note:** If you are configuring the router from a wireless computer and you change the router's SSID, channel, or security settings, you will lose your wireless connection when you click Apply. You must then change the wireless settings of your computer to match the router's new settings.

8. In the main menu of the WNR834B router, under the heading Advanced, click Wireless Settings**.**

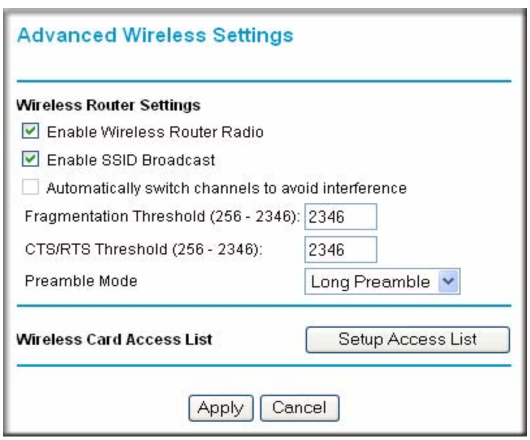


Figure 8-2

9. Make sure the checkboxes are selected for Enable Wireless Router Radio and Enable SSID Broadcast.
10. Click Setup Access List.
11. Make sure that the checkbox is *not* selected for Turn Access Control On.
12. Configure and test your wireless computer for wireless connectivity.

Program the wireless adapter of your computer to have the same SSID and channel that you configured in the router, and disable encryption. Check that your computer has a wireless link and is able to obtain an IP address by DHCP from the router.

Once your computer has basic wireless connectivity to the router, you can configure the advanced wireless security functions of the computer and router.

Restoring the Default Configuration and Password

This section explains how to restore the factory default configuration settings, changing the router's administration password back to **password**. You can erase the current configuration and restore factory defaults in two ways:

- Use the Erase function of the router (see "Erasing the Configuration" on page 7-8).
- Use the Default Reset button on the rear panel of the router. Use this method for cases when the administration password or IP address is not known.

To restore the factory default configuration settings without knowing the administration password or IP address, you must use the Default Reset button on the rear panel of the router.

1. Press and hold the Default Reset button for 10 seconds.

2. Release the Default Reset button and wait for the router to reboot.

If the wireless router fails to restart or the power light continues to blink or turns solid amber, the unit may be defective. If the error persists, you might have a hardware problem and should contact technical support at *www.netgear.com/support*.

Appendix A
Technical Specifications

This appendix provides technical specifications for the WNR834B wireless router.

Factory Default Settings

When you first receive your WNR834B, the default factory settings are in effect, as shown below. You can restore these defaults with the Factory Default Restore button on the rear panel.

Router Login Default Access	
Router Login URL	http://www. routerlogin.net *or* http://www.routerlogin.com
Login Name (case sensitive) printed on product label	admin
Login Password (case sensitive) printed on product label	password
Internet Connection	
WAN MAC Address	Use default hardware address
MTU Size	1500
Local Network	
Router LAN IP address printed on product label (also known as Gateway IP address)	www.routerlogin.net or `192.168.1.1`
Router Subnet	`255.255.255.0`
DHCP Server	Enabled
DHCP range	`192.168.1.2` to `192.168.1.254`
Time Zone	Pacific Time
Time Zone Adjusted for Daylight Saving Time	Disabled

Wireless	
Wireless Router Radio	Enabled
Wireless Access List (MAC Filtering)	All wireless stations allowed
SSID	NETGEAR
802.11b/g RF Channel	Auto
Mode	Up to 240 Mbps
Wireless Security	None
Firewall	
Inbound (communications coming in from the Internet)	Disabled (bars all unsolicited requests)
Outbound (communications going out to the Internet)	Enabled (all)

General Specifications

Network Protocol and Standards Compatibility	
Data and Routing Protocols:	TCP/IP, RIP-1, RIP-2, DHCP, PPPoE, PPTP, Bigpond, Dynamic DNS, and UPnP
Power Adapter	
North America:	120V, 60 Hz, input
UK, Australia:	240V, 50 Hz, input
Europe:	230V, 50 Hz, input
Japan:	100V, 50/60 Hz, input
All regions (output):	12 V DC @ 1.0A output
Physical	
Dimensions:	9" x 6.8" x 3" 228.5 x 175 x 76 mm
Weight:	1.1 lbs. 0.5 kg
Environmental	
Operating temperature:	0° to 40° C (32º to 104º F)

Operating humidity:	90% maximum relative humidity, noncondensing
Electromagnetic Emissions	
Designed to conform to the following standards:	FCC Part 15 Class B; EN 55022/24 (CISPR 22/24) Class B; EN 60950 (CE LVD) Class B; MIC
Interface Specifications	
LAN:	10BASE-T or 100BASE-Tx, RJ-45
WAN:	10BASE-T or 100BASE-Tx, RJ-45

Appendix B
Related Documents

This appendix provides links to reference documents you can use to gain a more complete understanding of the technologies used in your NETGEAR product.

Document	Link
Internet Networking and TCP/IP Addressing	http://documentation.netgear.com/reference/enu/tcpip/index.htm
Wireless Communications	http://documentation.netgear.com/reference/enu/wireless/index.htm
Preparing a Computer for Network Access	http://documentation.netgear.com/reference/enu/wsdhcp/index.htm
Virtual Private Networking (VPN)	http://documentation.netgear.com/reference/enu/vpn/index.htm
Glossary	http://documentation.netgear.com/reference/enu/glossary/index.htm

In addition, you can find initial setup instructions for your wireless router in the *NETGEAR Wireless Router Setup Manual*.

Index